

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 1月29日
Date of Application:

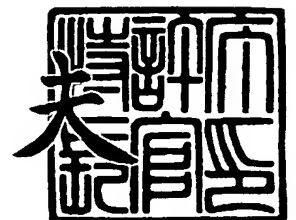
出願番号 特願2003-020937
Application Number:
[ST. 10/C]: [JP 2003-020937]

出願人 シャープ株式会社
Applicant(s):

2003年12月24日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



出証番号 出証特2003-3106951

【書類名】 特許願

【整理番号】 02J03829

【提出日】 平成15年 1月29日

【あて先】 特許庁長官 殿

【国際特許分類】 B41J 29/38
G03G 21/00
G06F 3/12
G06F 15/16

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

【氏名】 朝田 直樹

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

【氏名】 山下 博

【特許出願人】

【識別番号】 000005049

【氏名又は名称】 シャープ株式会社

【代理人】

【識別番号】 100080034

【弁理士】

【氏名又は名称】 原 謙三

【電話番号】 06-6351-4384

【選任した代理人】

【識別番号】 100113701

【弁理士】

【氏名又は名称】 木島 隆一

【選任した代理人】

【識別番号】 100116241

【弁理士】

【氏名又は名称】 金子 一郎

【手数料の表示】

【予納台帳番号】 003229

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0208489

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法

【特許請求の範囲】

【請求項 1】

ネットワークを介してデータを送信する電子機器と、該電子機器から送信されたデータを記憶する複数の記憶手段と、該記憶手段から上記データを取得して処理を行う複数の外部機器とが、ネットワークを介して互いに接続されている電子機器ネットワークシステムにおいて、

上記電子機器、記憶手段および外部機器は、それぞれがセキュリティ機能を有していることを特徴とする電子機器ネットワークシステム。

【請求項 2】

上記電子機器、記憶手段および外部機器が有しているセキュリティ機能のセキュリティレベルに応じて、上記電子機器、記憶手段および外部機器を検索する検索手段を備えていることを特徴とする請求項 1 に記載の電子機器ネットワークシステム。

【請求項 3】

上記外部機器の設置場所または外部機器が備えている機能に基づいて、上記外部機器の検索を行う検索手段を備えていることを特徴とする請求項 1 または 2 に記載の電子機器ネットワークシステム。

【請求項 4】

上記検索手段は、上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することを特徴とする請求項 2 または 3 に記載の電子機器ネットワークシステム。

【請求項 5】

上記外部機器は、自機のセキュリティレベルに対応する記憶手段を検索する検索部を備えていることを特徴とする請求項 1 ～ 4 の何れか 1 項に記載の電子機器ネットワークシステム。

【請求項 6】

上記電子機器は、上記検索手段による検索条件を入力し、該検索結果を表示する表示手段を備えていることを特徴とする請求項 1～5 の何れか 1 項に記載の電子機器ネットワークシステム。

【請求項 7】

上記電子機器、記憶手段および外部機器のセキュリティ機能は、アクセス制御手段を介して接続された複数のネットワークのうち、どのネットワークに配置されているかによって付与されることを特徴とする請求項 1～6 の何れか 1 項に記載の電子機器ネットワークシステム。

【請求項 8】

上記外部機器は、画像形成装置であることを特徴とする請求項 1～7 の何れか 1 項に記載の電子機器ネットワークシステム。

【請求項 9】

上記電子機器は、スキャナ装置であることを特徴とする請求項 1～8 の何れか 1 項に記載の電子機器ネットワークシステム。

【請求項 10】

ネットワークを介してデータを送信する電子機器と、該電子機器から送信されたデータを記憶する複数の記憶手段と、該記憶手段から上記データを取得して処理を行う複数の外部機器とが、ネットワークを介して互いに接続されている電子機器ネットワークシステムにおけるデータ送信方法において、

上記電子機器、記憶手段および外部機器は、それぞれセキュリティ機能を有しており、

上記電子機器からデータを送信する場合には、ユーザが設定したセキュリティレベルに応じて、該セキュリティレベルに適合するセキュリティ機能を備えた上記記憶手段および外部機器の検索を行うことを特徴とする電子機器ネットワークシステムによるデータ送信先検索方法。

【請求項 11】

上記外部機器の検索は、外部機器の設置場所、機能に基づいて行われることを特徴とする請求項 10 に記載の電子機器ネットワークシステムによるデータ送信先検索方法。

【請求項 12】

上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することを特徴とする請求項 10 または 11 に記載の電子機器ネットワークシステムによるデータ送信先検索方法。

【請求項 13】

セキュリティレベルが合致しない上記電子機器、上記記憶手段および上記外部機器に対するデータの送信を禁止することを特徴とする請求項 10～12 の何れか 1 項に記載の電子機器ネットワークシステムによるデータ送信先検索方法。

【請求項 14】

上記外部機器から上記記憶手段に格納されたデータを取り出す際に、必要なデータが格納されている記憶手段とセキュリティレベルが合致せずに該外部機器に対してデータを送信できない場合には、

上記検索手段が、上記必要なデータが格納されている記憶手段とセキュリティレベルが適合する外部機器を検索することを特徴とする請求項 13 に記載の電子機器ネットワークシステムによるデータ送信先検索方法。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、複数の電子機器がネットワークを介して接続されて構成されており、各電子機器から送信されるデータに基づいて、他の電子機器において出力する電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法に関するものである。

【0002】**【従来の技術】**

情報処理機器の発展およびインターネット環境の急速な充実に伴い、旧来の LAN 環境で用いられている技術に加え、インターネットで利用される様々な技術を適用した OA 機器が開発されている。

【0003】

このような OA 機器を使用すれば、各々の機器の個別利用にとどまらず、複数

の機能を組み合わせて利用することも可能になる。また、このようなOA機器は、コンピュータ機器の外部装置として利用されるだけでなく、逆にコンピュータ機器を外部装置として利用することも可能である。すなわち、OA機器は高度情報処理機器としての側面を備えており、オフィスにおける知的生産作業を支援するサービスを提供する機器となりつつある。

【0004】

このような情報処理機器の発展に伴い、1998年5月に設立されたOAシステム機器プロジェクト委員会は、OA機器の新たな統合インターフェース仕様としてBMLinkSを開発した。

【0005】

このBMLinkSの規格として、ホストコンピュータ（ホストPC）から送信した印刷データをストレージサーバに格納し、この格納した印刷データをストレージサーバからプリンタに送信して印刷出力する印刷システムがある。

【0006】

また、ネットワーク上に情報処理装置やプリンタ等が分散配置された印刷システムにおいて、印刷データを出力するためのプリンタを検索して、検索されたプリンタに印刷データを送信し、出力させるといったプリントシステムがある（特許文献1参照）。

【0007】

特許文献1では、ユーザが作成した印刷ジョブに適した機能（用紙サイズ、両面印刷、ソート等）やフォーマット（ビットマップ、プリンタ言語等）を検索し、出力するプリントシステムが提案されている。

【0008】

ネットワークやインターネットが急速に発展している昨今、上述のような印刷システムは非常に便利なものであり、利用価値が高い。

【0009】

しかし、上記特許文献1に開示されたプリントシステムは、印刷データの保護（セキュリティ）という観点に立って構築されていない。このため、機密文書などを印刷する場合に、データ漏洩などの危険性があり、安易に利用することがで

きない。

【0010】

そこで、印刷データのパスワードを付加し、そのパスワードを入力して印刷出力や印刷データの削除を可能にすることで、印刷データの漏洩等の問題を解決した印刷システムがある（特許文献2・3参照）。

【0011】

例えば、特許文献2に開示されたデータ出力制御システムでは、セキュリティ印刷モードに設定されると、プリントサーバにおいて、IDおよびパスワードが照合されない限り、印刷データをプリント装置へ出力しないように制御することで、データ漏洩等の問題を解決している。

【0012】

【特許文献1】

特開平07-214872号公報（公開日1995年8月15日）

【0013】

【特許文献2】

特開平10-021022号公報（公開日1998年1月23日）

【0014】

【特許文献3】

特開平11-301058号公報（公開日1999年11月2日）

【0015】

【発明が解決しようとする課題】

しかしながら、上記特許文献2に開示されたシステムでは、IDおよびパスワードの入力により安全性を確保しているが、IDおよびパスワードが分からないユーザにはセキュリティ印刷モードでプリンタの利用ができないという問題を有している。

【0016】

本発明は、上記の問題点に鑑みてなされたものであり、その目的は、ネットワークを構成する電子機器間において送信されるデータの保護（セキュリティ）を考慮しつつ、ユーザが自由にセキュリティレベルに応じた送信ルートでデータの

送信を行うことが可能な電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法を提供することにある。

【0017】

【課題を解決するための手段】

本発明の電子機器ネットワークシステムは、上記の課題を解決するために、ネットワークを介してデータを送信する電子機器と、該電子機器から送信されたデータを記憶する複数の記憶手段と、該記憶手段から上記データを取得して処理を行う複数の外部機器とが、ネットワークを介して互いに接続されている電子機器ネットワークシステムにおいて、上記電子機器、記憶手段および外部機器は、それぞれがセキュリティ機能を有していることを特徴としている。

【0018】

上記の構成によれば、電子機器から記憶手段を介して外部機器へデータを送信する場合には、ユーザが希望するセキュリティレベルに対応するセキュリティ機能を有する記憶手段および外部機器を選択することで、データを安全かつ容易に記憶手段および外部機器に対して送信できる。

【0019】

すなわち、本発明の電子機器ネットワークシステムは、電子機器と、各種データが記憶（格納）される記憶手段と、記憶手段に格納されたデータを取得して処理を行う外部機器とが、ネットワークを介して互いに接続されており、例えば、BMLinkS等の規格に適合した構成である。

【0020】

電子機器は、例えば、ホストPCやスキャナ装置等であって、ネットワークを介して、記憶手段、外部機器に対してデータを送信する。

【0021】

記憶手段は、例えば、ネットワーク内に設けられたストレージサーバ等であって、それぞれ個別のセキュリティレベルが設定されている。

【0022】

外部機器は、例えば、プリンタ、MFP（MultiFunction Printer）等であって、送信されたデータの処理を行う。

【0023】

本発明の電子機器ネットワークシステムでは、上記電子機器、記憶手段および外部機器のそれぞれがセキュリティ機能を備えている。

【0024】

このセキュリティ機能は、例えば、データ通信時に用いる暗号化プロトコルであってもよいし、イントラネットとインターネットとを組み合わせたネットワークを形成することでセキュリティ機能を付与してもよい。また、セキュリティレベルは、例えば、0, 1, 2 という3段階で設定してもよい。なお、セキュリティレベル0とは、データのセキュリティについて何も考慮されていない状態でデータの送受信を行うことをいう。

【0025】

これにより、ユーザは、送信するデータの重要度に応じてセキュリティレベルを設定し、該セキュリティレベルに基づいてデータを出力する外部機器までのデータ送信ルートを検索することで、ユーザは安全かつ確実にデータを所望の記憶手段あるいは外部機器に対して送信できる。

【0026】

例えば、ユーザにとって重要度の高いデータを送信する場合には、セキュリティレベルが「高」である記憶手段と外部機器とを組み合わせたデータ送信ルートに沿ってデータを送信することにより、第三者にデータが漏洩する等の問題を解決できる。

【0027】

よって、ユーザは、重要なデータを安全に送信したい場合には、IDやパスワードを入力することなく、単に、所望のセキュリティレベルに合致した記憶手段および外部機器を選択するだけで、データの安全性を確保した電子機器ネットワークシステムを実現することが可能となる。

【0028】

上記電子機器、記憶手段および外部機器が有しているセキュリティ機能のセキュリティレベルに応じて、上記電子機器、記憶手段および外部機器を検索する検索手段を備えていることがより好ましい。

【0029】

これにより、ユーザは送信するデータの重要度に応じて、セキュリティレベルを設定するだけで、ネットワークに接続された複数の記憶手段、外部機器の中から、設定されたセキュリティレベルに対応する記憶手段および外部機器を容易に検索することができる。

【0030】

よって、ユーザは、所望のセキュリティレベルのセキュリティ機能を有する記憶手段と外部機器とを組み合わせたルートに沿って、データを安全に送信することができる。

【0031】

上記外部機器の設置場所または外部機器が備えている機能に基づいて、上記外部機器の検索を行う検索手段を備えていることがより好ましい。

【0032】

これにより、ユーザは、データを出力する外部機器が設置されている場所や外部機器が備えている機能に基づいて外部機器を検索することができるため、ネットワークに接続された複数の外部機器の中から、ユーザの希望に沿った外部機器をより容易に選択することができる。

【0033】

例えば、ユーザがデータの出力を希望する地域が決まっている場合には、まず、外部機器の設置場所を入力して外部機器を検索し、該検索結果に対してさらにセキュリティレベル、外部機器が備えている機能等の条件に基づいて検索することで、ユーザの希望に沿う外部機器の検索が可能になる。

【0034】

また、送信されるデータの処理が特殊である場合には、外部機器の機能に基づいてその処理を行う機能を備えた外部機器を検索することができ、より詳細な検索が可能になる。

【0035】

上記検索手段は、上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することがより好ましい。

【0036】

これにより、ユーザは、所望のセキュリティレベルあるいは外部機器の設置場所、機能等に基づいて、電子機器から記憶手段を介して外部機器に至るまでのデータの送信ルートを検索することができる。

【0037】

例えば、ユーザがセキュリティレベル「高」でのデータ送信を希望する場合には、セキュリティレベルが「高」以上のセキュリティ機能を備えた記憶手段および外部機器を検索し、これらを組み合わせた送信ルートを検索結果として表示する。

【0038】

よって、ユーザ所望のセキュリティレベルに応じて別々に検索した記憶手段および外部機器を組み合わせて送信ルートを決定する場合と比較して、効率よく所望のセキュリティレベルに適合する送信ルートを見つけることができる。

【0039】

上記外部機器は、自機のセキュリティレベルに対応する記憶手段を検索する検索部を備えていることがより好ましい。

【0040】

これにより、ユーザが操作している外部機器においても、その外部機器に対してデータの送信が可能なセキュリティ機能を有する記憶手段を検索することができるため、ユーザは外部機器において、直接データが格納されている記憶手段から必要なデータを取得することが可能になる。

【0041】

よって、外部機器において、記憶手段からデータを取得する場合でも、データの安全性を考慮した出力が可能になる。

【0042】

また、ユーザが操作中の外部機器に対してデータを送信することができる記憶手段を検索することで、セキュリティレベルが合わないため、記憶手段に格納されたデータを目的とする外部機器から取り出すことができないといった問題を未然に防止することができる。

【0043】

上記電子機器は、上記検索手段による検索条件を入力し、該検索結果を表示する表示手段を備えていることがより好ましい。

【0044】

これにより、ユーザは検索条件を容易に入力できるとともに、検索結果としてセキュリティレベル、ストレージの使用料金、外部機器の設置場所、外部機器の機能等を表示することができ、ユーザの操作性を向上することができる。

【0045】

上記電子機器、記憶手段および外部機器のセキュリティ機能は、アクセス制御手段を介して接続された複数のネットワークのうち、どのネットワークに配置されているかによって付与されることがより好ましい。

【0046】

これにより、例えば、ルータ、ファイアウォール等のアクセス制御手段を介して接続された企業内のイントラネットと外部の誰からもアクセスが可能なインターネットとを組み合わせることで、上記企業の社員から見て、3段階のセキュリティレベルを設定することができる。具体的には、企業内に形成されたイントラネットのみに接続可能な機器等はセキュリティレベルを「高」、両方のネットワークに接続可能な機器等はセキュリティレベルを「中」、そしてインターネットのみに接続可能な機器等がセキュリティレベルを「低」とすることができる。

【0047】

よって、ユーザは、重要なデータについては、社内のイントラネットのみに接続可能な機器を用いて印刷データを送信、出力することで、インターネットにしか接続できない外部の機器に対してデータが漏洩することを防止し、安全かつ確実にデータを出力することができる。

【0048】

上記外部機器は、画像形成装置であることがより好ましい。

【0049】

これにより、ホストPC等の電子機器から送信された印刷データを、ネットワークに接続された複数の記憶手段、外部機器の中から、ユーザ所望のセキュリテ

イレベルに適合した記憶手段、画像形成装置に対して送信することができるため、データの安全性を確保した印刷システムを構築できる。

【0050】

上記電子機器は、スキャナ装置であることがより好ましい。

【0051】

これにより、スキャナ装置で読み取った画像データ等を、記憶手段、外部機器あるいは他の電子機器に対して安全に送信することが可能なスキャナシステムを構築できる。

【0052】

本発明の電子機器ネットワークシステムによるデータ送信先検索方法は、上記の課題を解決するために、ネットワークを介してデータを送信する電子機器と、該電子機器から送信されたデータを記憶する複数の記憶手段と、該記憶手段から上記データを取得して処理を行う複数の外部機器とが、ネットワークを介して互いに接続されている電子機器ネットワークシステムにおけるデータ送信方法において、上記電子機器、記憶手段および外部機器は、それぞれセキュリティ機能を有しており、上記電子機器からデータを送信する場合には、ユーザが設定したセキュリティレベルに応じて、該セキュリティレベルに適合するセキュリティ機能を備えた上記記憶手段および外部機器の検索を行うことを特徴としている。

【0053】

上記の方法によれば、ネットワークを介して複数の電子機器、記憶手段および外部機器がそれぞれ分散配置されたBMLinkS等に適合した電子機器ネットワークシステムにおいて、ユーザが希望するセキュリティレベルに応じて、適合する記憶手段および外部機器を検索できるため、ネットワークに接続された多数の記憶手段および外部機器の中から、安全にデータを送信できる記憶手段および外部機器を容易に見つけることができる。

【0054】

すなわち、本発明に係る電子機器ネットワークシステムは、電子機器と、各種データが記憶（格納）される記憶手段と、記憶手段に格納されたデータを取得して処理を行う外部機器とが、ネットワークを介して互いに接続されており、例え

ば、BMLinkS等の規格に適合した構成である。

【0055】

電子機器は、例えば、ホストPCやスキャナ装置等であって、ネットワークを介して、記憶手段、外部機器に対してデータを送信する。

【0056】

記憶手段は、例えば、ネットワーク内に設けられたストレージサーバ等であって、それぞれ個別のセキュリティレベルが設定されている。

【0057】

外部機器は、例えば、プリンタ、MFP (MultiFunction Printer) 等であって、送信されたデータの処理を行う。

【0058】

また、本発明に係る電子機器ネットワークシステムでは、上記電子機器、記憶手段および外部機器のそれぞれがセキュリティ機能を備えている。

【0059】

このセキュリティ機能は、例えば、暗号化プロトコルを用いたデータ通信であってもよいし、イントラネットおよびインターネットを組み合わせたネットワークを形成することでセキュリティ機能を付与してもよい。また、セキュリティレベルは、例えば、0, 1, 2という3段階に設定してもよい。なお、セキュリティレベル0とは、データのセキュリティについて何も考慮されていない状態でデータの送受信を行うことをいう。

【0060】

これにより、ユーザは、送信するデータの重要度に応じて、データを出力する外部機器までのデータ送信ルートを検索することで、ユーザは安心してデータを外部機器まで送信できる。

【0061】

例えば、ユーザにとって重要度の高いデータを送信する場合には、セキュリティレベルの高い記憶手段と、該セキュリティレベルの高い記憶手段からデータを取得して出力可能なセキュリティレベルの外部機器とを組み合わせたデータ送信ルートに沿ってデータを送信することにより、第三者にデータが漏洩する等の問

題を解決できる。

【0062】

よって、ユーザは、重要なデータを安全に送信したい場合には、IDやパスワードを入力することなく、単に、所望のセキュリティレベルに合致した記憶手段および外部機器を選択するだけで、データの安全性を確保した電子機器ネットワークシステムを実現することが可能となる。

【0063】

上記外部機器の検索は、外部機器の設置場所、機能に基づいて行われることがより好ましい。

【0064】

これにより、ユーザは、データを出力する外部機器が設置されている場所や外部機器が備えている機能に基づいて外部機器を検索することができるため、ネットワークに接続された複数の外部機器の中から、ユーザの希望に沿った外部機器をより容易に選択することができる。

【0065】

例えば、ユーザがデータの出力を希望する地域が決まっている場合には、まず、外部機器の設置場所を入力して外部機器を検索し、該検索結果に対してさらにセキュリティレベル、外部機器が備えている機能等の条件に基づいて検索することで、ユーザの希望に沿う外部機器の検索が可能になる。

【0066】

また、送信されるデータの処理が特殊である場合には、外部機器の機能に基づいてその処理を行う機能を備えた外部機器を検索することができ、より詳細な検索が可能になる。

【0067】

上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することがより好ましい。

【0068】

これにより、ユーザは、所望のセキュリティレベル、外部機器の設置場所、機能等に基づいて、電子機器から記憶手段を介して外部機器に至るまでのデータの

送信ルートを検索することができる。

【0069】

例えば、ユーザがセキュリティレベル「高」でのデータ送信を希望する場合には、セキュリティレベルが「高」以上のセキュリティ機能を備えた記憶手段および外部機器を検索し、これらを組み合わせた送信ルートを検索結果として表示する。

【0070】

よって、ユーザ所望のセキュリティレベルに応じて別々に検索した記憶手段および外部機器を組み合わせて送信ルートを決定的する場合と比較して、効率よく所望のセキュリティレベルに適合する送信ルートを見つけることができる。

【0071】

セキュリティレベルが合致しない上記電子機器、上記記憶手段および上記外部機器に対するデータの送信を禁止することがより好ましい。

【0072】

これにより、ユーザが安全性を重視してデータ送信を行いたい場合でも、誤って誰でもアクセス可能な記憶手段や、誰でも利用可能な外部機器にデータが送信されることを防止でき、より確実にセキュリティ機能を持った所望の外部機器に対してデータを送信できる。

【0073】

上記外部機器から上記記憶手段に格納されたデータを取り出す際に、必要なデータが格納されている記憶手段とセキュリティレベルが合致せずに該外部機器に対してデータを送信できない場合には、上記検索手段が、上記必要なデータが格納されている記憶手段とセキュリティレベルが適合する外部機器を検索することがより好ましい。

【0074】

これにより、ユーザがある外部機器から、記憶手段に格納されているデータを取り出して出力する場合であって、必要なデータが格納されている記憶手段とセキュリティレベルが合致しない場合には、検索手段が該外部機器に対して出力可能な外部機器を検索することができる。

【0075】

よって、ユーザは常に必要なデータを取り出せる外部機器を把握して、必要なデータをセキュリティレベルの合致した外部機器から出力することができる。

【0076】**【発明の実施の形態】****〔実施形態1〕**

本発明の電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法の一実施形態に係る印刷システムについて、図1～図11を用いて説明すれば以下のとおりである。

【0077】

本実施形態の印刷システムは、複数のホストPC（電子機器）、複数のストレージ（記憶手段）および複数のプリンタ（外部機器）を備え、それぞれがインターネットを介して接続されたネットワークを構成している。

【0078】

具体的には、図2に示すように、3台のホストPC（ホストHA11、ホストHB12、ホストHC13）、3つのストレージ（ストレージSA21、ストレージSB22、ストレージSC23）、4台のプリンタ（プリンタPA31、プリンタPB32、プリンタPC33、プリンタPD34）、および検索サーバ（検索手段）41とを備えている。

【0079】

ホストPC11～14は、例えば、パーソナルコンピュータ、ワークステーション等の一般的なコンピュータであって、プリンタ31～34に対して印刷データを送信する。

【0080】

ストレージ21～23は、ホストPC11～14から送信された各種データを記憶（格納）している。本実施形態のストレージ21～23は、特に、ホストPC11～14から送信された印刷データを一時的に保管し、必要に応じてプリンタ31～34へ出力する。

【0081】

プリンタ 31～34 は、ストレージ 21～23 から送信された、あるいはホスト PC 11～14 から直接送信された印刷データの出力処理、つまり印刷を行う。

【0082】

検索サーバ 41 は、各ストレージ 21～23 および各プリンタ 31～34 が有する各種の機能に基づいて、目的とするストレージ 21～23 あるいはプリンタ 31～34 を検索することができる。より具体的には、あるデータについて両面印刷で出力処理を行いたい場合に、この検索サーバ 41 において、両面印刷機能を有しているプリンタ 31～34 を検索することができる。なお、この検索サーバ 41 は、各ストレージ 21～23 および各プリンタ 31～34 のセキュリティレベルについても検索することができる。

【0083】

ここで、各ホスト 11～14、各ストレージ 21～23 および各プリンタ 31～34 に付与されたセキュリティ機能について説明する。

【0084】

本実施形態の印刷システムでは、各ホスト PC 11～14、各ストレージ 21～23 および各プリンタ 31～34 に対して、「暗号化プロトコル 2.0」、「暗号化プロトコル 1.0」、「暗号化プロトコルなし」という 3 種類のデータ保護機能を各機器ごとに付与することで、「高」、「中」、「低」の 3 段階のセキュリティレベルを実現している。

【0085】

なお、セキュリティ機能を付与する方法としては、暗号化プロトコルを用いた方法に限定されるものではなく、例えば、実施形態 2 で説明するイントラネットとインターネットとを組み合わせる付与方法や、実施形態 3 で説明する暗号化手段でデータを暗号化した状態で送信する方法であってもよい。

【0086】

続いて、ホスト PC 11～14、ストレージ 21～23、プリンタ 31～34、検索サーバ 41 のより詳細な構成について、図 1 を用いて説明する。

【0087】

各ストレージ 21～23 は、図 1 に示すように、通信部 211、制御部 212、ストレージ情報記憶部 213、暗号・復号化部 214 および印刷データ記憶部 215 を備えている。

【0088】

通信部 211 は、外部の各機器とのデータの送受信を行うインターフェース部である。

【0089】

制御部 212 は、装置全体を制御する装置の中心となる部分である。

【0090】

ストレージ情報記憶部 213 には、例えば、セキュリティレベル、使用料金などのストレージ情報が記憶されている。なお、ここに記憶されている情報については、図示しない表示手段によって表示され、ユーザが確認することができる。

【0091】

暗号・復号化部 214 は、ストレージ 21～23 に格納される印刷データを保護するために、ホスト PC 11～14 から送信された印刷データの内容が、第三者によって容易に読み取られないように、印刷データの暗号化処理を行うとともに、暗号化されている印刷データを読み取り可能な状態に復元する復号化処理も行う。

【0092】

印刷データ記憶部 215 は、上記暗号・復号化部 214 によって処理された印刷データを格納している。

【0093】

プリンタ 31～34 は、それぞれに、通信部 311、制御部 312、プリンタ情報記憶部 313、暗号・復号化部 314、画像形成部 315 および検索部 316 を備えている。

【0094】

通信部 311 は、外部の各機器とのデータの送受信を行うインターフェース部である。

【0095】

制御部 312 は、装置全体を制御する装置の中心となる部分である。

【0096】

プリンタ情報記憶部 313 は、自プリンタのプリンタ情報（例えば、セキュリティレベル、印刷機能など）を記憶している。なお、ここに記憶されている情報についても、図示しない表示手段によって表示され、ユーザが確認することができる。

【0097】

暗号・復号化部 314 は、上記ストレージ 21～23 が備えている暗号・復号化部 214 と同様に、印刷データの暗号化処理を行うとともに、暗号化されている印刷データを読み取り可能な状態に復元する復号化処理も行う。

【0098】

画像形成部 315 は、暗号・復号化部 314 によって復元された印刷データに基づいて画像形成を行う。

【0099】

検索部 316 は、自プリンタに対して出力可能なストレージを検索する。

【0100】

ホスト PC 11～14 は、それぞれ、通信部 111、制御部 112、ホスト情報記憶部 113、暗号・復号化部 114、検索ドライバ 115 およびプリンタドライバ 116 を備えている。

【0101】

通信部 111 は、外部の各機器とのデータの送受信を行うインターフェース部である。

【0102】

制御部 112 は、装置全体を制御する装置の中心となる部分である。

【0103】

ホスト情報記憶部 113 は、セキュリティレベルなどの自ホストのホスト情報を記憶している。なお、ここに記憶されている情報についても、図示しない表示手段によって表示され、ユーザが確認することができる。

【0104】

暗号・復号化部 114 は、上記暗号・復号化部 214・314 と同様に、印刷データの暗号化処理を行うとともに、暗号化されている印刷データを読み取り可能な状態に復元する復号化処理も行う。

【0105】

検索ドライバ 115 は、検索サーバ 41 を駆動するための駆動手段であり、これを用いることで、ホスト PC 11～14 において、検索サーバ 41 を利用して目的とする機器の検索を行うことができる。

【0106】

プリンタドライバ 116 は、ホスト PC 11～14 にインストールされているアプリケーションを用いてユーザが作成したデータを、各プリンタ用のプリントデータに変換したり、処理を依頼するプリンタに対して所望の印刷条件（部数、用紙サイズ等）で印刷処理を行わせたりする。さらに、プリンタドライバ 116 は、プリントデータ（プリントジョブ）をストレージ 21～23 へ記憶させる役割も担う。

【0107】

検索サーバ 41 は、通信部 411、制御部 412、機器情報記憶部 413 および検索部 414 を備えている。

【0108】

通信部 411 は、外部の各機器とのデータの送受信を行うインターフェース部である。

【0109】

制御部 412 は、検索サーバ 41 を制御する装置の中心となる部分である。

【0110】

機器情報記憶部 413 は、本ネットワークにおける全ての機器に関する情報、例えば、各プリンタやストレージのセキュリティレベル、各プリンタの印刷機能等を記憶している。なお、ここに記憶されている情報についても、ホスト PC の図示しない表示部によって表示され、ユーザに確認させることができる。

【0111】

検索部 414 は、ユーザから指定された検索内容に応じて、ネットワーク上の

各機器から情報を取得した機器情報記憶部 413 に記憶されている機器情報に基づいて、ユーザ所望のセキュリティ機能を有するホスト PC 11～14、ストレージ 21～23 あるいはプリンタ 31～34 の検索を行う。

【0112】

各ストレージ 21～23、各プリンタ 31～34、各ホスト PC 11～14、検索サーバ 41 にそれぞれ設けられている各情報記憶部 113・213・313・413 は、図 3 (a)～図 3 (d) に示すように、各種情報を記憶している。

【0113】

ストレージ 21～23 がそれぞれ備えているストレージ情報記憶部 213 は、図 3 (a) に示すように、ストレージ名、ストレージ使用料金およびセキュリティレベル（データ保護機能）を記憶している。

【0114】

ストレージ SA 21 は、セキュリティレベルが「高」であり、印刷データを暗号化して送信することができる暗号化プロトコル 2.0、およびサーバトラブル時対策のためのバックアップ機能を備えている。

【0115】

ストレージ SB 22 は、セキュリティレベルが「中」であり、印刷データを暗号化して送信することができる暗号化プロトコル 1.0 を備えている。

【0116】

また、ストレージサーバ SC 23 は、セキュリティレベルが「低」であって、データ保護目的の機能を特に備えていない。

【0117】

本実施形態の印刷システムでは、以上のように、データ保護に関するセキュリティレベルの異なる 3 つのストレージを備えている。

【0118】

ここで、セキュリティレベル「高」とは、ネットワーク的にも、物理的にもデータ保護の観点から安全性が高いストレージを意味する。このセキュリティレベル「高」のストレージとしては、例えば、会社内のイントラネット上にある機器（パソコン、プリンタなど）としか接続できないストレージがある。

【0119】

セキュリティレベル「中」とは、ネットワーク的な面では安全性に問題があるが、物理的には安全性が高いストレージを意味する。このセキュリティレベル「中」のストレージとしては、例えば、会社内に設置されているが、社外のインターネット上にある機器と接続できるストレージがある。

【0120】

セキュリティレベル「低」のストレージとは、ネットワーク的な面からも、物理的な面からもデータ保護の面である程度の危険性を有するストレージを意味する。このセキュリティレベル「低」のストレージとしては、例えば、インターネット上で誰でもアクセス可能なストレージサービスがある。

【0121】

なお、上述したイントラネット、インターネット等を組み合わせてセキュリティ機能が付与されたストレージを備えた印刷システムについては、後述する実施形態2において詳しく説明する。

【0122】

上記のように、各ストレージ21～23は、そのセキュリティレベルに差があるため、使用料金について、そのセキュリティレベルに応じて高いものから順に200円、100円、無料と設定されている。

【0123】

各プリンタ31～34のプリンタ情報記憶部313は、図3（b）に示すように、プリンタ名、各プリンタ31～34のセキュリティレベルを示すデータ保護機能、プリンタの設置場所およびプリンタが備えている印刷機能について記憶している。

【0124】

プリンタPA31は、暗号化プロトコル2.0および1.0、および印刷される直前まで暗号化された状態で印刷データをストックすることができるよう復号化機能を備えており、セキュリティレベルは「特高」である。

【0125】

プリンタPB32は、暗号化プロトコル2.0および1.0を備えており、セ

キュリティレベルは「高」である。

【0126】

プリンタPC33は、暗号化プロトコル1.0のみを備えており、セキュリティレベルは「中」である。

【0127】

プリンタPD34は、データ保護目的の機能を特に備えておらず、セキュリティレベルは「低」である。

【0128】

また、プリンタ情報記憶部313は、各プリンタの設置場所および各プリンタが備えているカラー、両面、ステープル等の印刷機能に関する情報も記憶している。この記憶情報については、各プリンタの図示しない表示部、あるいは検索サーバ41を介して、各ホストPCから確認することができる。

【0129】

各ホストPC11～14のホスト情報記憶部113は、図3(c)に示すように、ホスト名と、各ホストPC11～14のセキュリティレベルを示すデータ保護機能とに関する情報を記憶している。

【0130】

本実施形態の各ホストPC11～14は、印刷データを暗号化して送信することができる暗号化プロトコル2.0および1.0を全て備えており、セキュリティレベル「低」、「中」、「高」の全てのレベルに対応可能である。

【0131】

検索サーバ41の機器情報記憶部413は、図3(d)に示すように、ストレージ名、接続可能なプリンタおよびセキュリティレベルに関する情報を記憶している。

【0132】

これらの情報は、検索サーバ41が、各プリンタ31～34からプリンタ情報、各ストレージ21～23からストレージ情報をそれぞれ収集することにより取得してもよいし、予め作成された情報を記憶しておいてもよい。

【0133】

本実施形態の印刷システムにおいては、検索サーバ41がこのような機器情報記憶部413を備えていることにより、各印刷データに対して付与すべきセキュリティレベルに応じて、各種機器（ストレージ21～23、プリンタ31～34）を選択することができる。

【0134】

なお、検索サーバ41には、図4（a）～図4（c）に示すように、各セキュリティレベルに応じて、ストレージとプリンタとを組み合わせた印刷ルートを検索する図示しないルート検索部（ルート検索手段）が設けられていてもよい。

【0135】

例えば、ユーザ所望のセキュリティレベルが「高」以上（「特高」または「高」）である場合には、検索サーバ41は、図4（a）に示すように、ストレージSA21と、プリンタPA31またはプリンタPB32とを組み合わせた印刷ルートを検索することができる。

【0136】

ユーザ所望のセキュリティレベルが「中」の場合には、図4（b）に示すように、ストレージSB22と、プリンタPA31またはプリンタPB32またはプリンタPC33とを組み合わせた印刷ルートを検索することができる。

【0137】

ユーザ所望のセキュリティレベルが「低」の場合には、検索サーバ41は、図4（c）に示すように、ストレージSC23と、プリンタ31～34のうちの任意のプリンタとを組み合わせた印刷ルートを検索することができる。

【0138】

本実施形態の印刷システムは、このように、ユーザが希望するセキュリティレベルに応じて、最適な送信ルートを容易に検索することができるため、データ保護のセキュリティ面を考慮してホストPC11～14から送信された印刷データをプリンタ31～34において出力することができる。

【0139】

次に、本実施形態の印刷システムにおいて、セキュリティレベルに応じた印刷データの送信方法について、図5および図6（a）～図6（d）を用いて説明す

れば以下のとおりである。

【0140】

なお、図6（a）～図6（d）は、各ホストPC11～14において、印刷処理を行う場合に表示される操作画面を示す模式図である。

【0141】

ホストPC11～14において印刷データ送信を開始する場合には、図5に示すように、S1において、最初にホストPC11～14の検索ドライバ115が起動する。これにより、S2において、該ホストPC11～14と検索サーバ41とが接続される。

【0142】

すると、ホストPC11～14には、図6（a）に示すような表示画面が現れ、検索カテゴリー（検索条件）を選択することができる。

【0143】

ここで、セキュリティレベルに応じた検索を行う場合には、S3において、「セキュリティ」ボタンを選択する。

【0144】

続いて、ホストPC11～14には、図6（b）に示すような表示画面が現れ、所望とするセキュリティレベル（その印刷データに付与したいセキュリティレベル）を選択することができる。なお、図6（b）には、セキュリティレベル「高」を選択した場合を示す。

【0145】

S4において、例えば、セキュリティレベル「高」が選択されると、S5において、図6（c）に示すように、目的とするセキュリティレベルに応じたストレージが表示される。

【0146】

そして、S6において、ユーザは図6（c）に示されるような3つのストレージから任意のストレージを選択する。なお、図6（c）には、ストレージSAが選択された場合を示す。

【0147】

S 6 において、ユーザが所望のストレージを選択すると、S 7 において、図 6 (d) に示すように、先に選択したストレージとセキュリティレベルとに応じて、印刷可能なプリンタが表示される。

【0 1 4 8】

ここで、表示された印刷可能プリンタの設置場所あるいは印刷機能が目的とするものでない場合、すなわち、S 8 において Y e s の場合には、再度 S 3 より操作をやり直すことができる。

【0 1 4 9】

一方、上記印刷可能プリンタの機能等が目的に適合したものである場合、すなわち、S 8 で N o の場合には、S 9 において、ストレージ使用料として課金処理が行われた後、S 1 0 において、印刷データが作成される。そして、S 1 1 において、該当するストレージへ暗号化プロトコルを利用して印刷データが送信される。

【0 1 5 0】

本実施形態の印刷システムでは、以上のように、ホスト P C からストレージに対して印刷データが送信されるため、印刷データのセキュリティレベルに応じたルートで送信処理を行うことができ、データ保護の観点から安全性の高い印刷システムを実現できる。

【0 1 5 1】

次に、本実施形態の印刷システムにおいて、印刷データを出力するプリンタの設置場所を優先して印刷データの送信ルートを決定する方法について、図 7 に示すフローチャートを用いて説明すれば以下のとおりである。

【0 1 5 2】

上述した印刷データの送信方法では、セキュリティレベルの設定を優先して印刷ルートを決定していたが、ここでは、印刷データの出力処理が行われるプリンタの設置場所の設定を優先して、プリンタとストレージとを組み合わせた印刷ルートを検索する。

【0 1 5 3】

ホスト P C 1 1 ~ 1 4 から印刷データの送信を開始する場合には、図 7 に示す

ように、S 2 1において、最初に、ホストPC 1 1～1 4内の検索ドライバ 1 1 5を起動し、S 2 2において、該ホストPC 1 1～1 4を検索サーバ 4 1に接続する。

【0 1 5 4】

すると、ホストPC 1 1～1 4における図示しない表示部には、図 8（a）に示すような表示画面が現れ、検索カテゴリー（検索条件）を選択することができる。ここで、印刷データを出力するプリンタの選択を優先して検索を行う場合には、S 2 3において、「プリンタ」ボタンを選択する。

【0 1 5 5】

続いて、ホストPC 1 1～1 4の表示部には、図 8（b）に示すような表示画面が現れ、ユーザは、S 2 4において、例えば、設置場所、機能などのプリンタの検索条件を入力する。なお、図 8（b）には、検索条件として、プリンタの設置場所（住所）を選択した場合を示す。

【0 1 5 6】

ここで、例えば、ユーザが、印刷を行いたいプリンタの設置場所（住所）として、奈良県を選択した場合には、S 2 5において、図 8（c）に示すように、奈良県内に設置されたプリンタの一覧が表示される。なお、この一覧には、プリンタの設置場所だけでなく、印刷機能およびセキュリティレベルについても表示される。

【0 1 5 7】

従って、ユーザは、S 2 6において、希望する設置場所およびその印刷データに見合った印刷機能およびセキュリティレベルを備えたプリンタを選択することができる。なお、S 2 6において、ユーザの希望に見合ったプリンタが一覧に表示されていない場合には、再度、S 2 3に戻って検索カテゴリーの選択からやり直すこともできる。

【0 1 5 8】

S 2 6において、プリンタが選択されると、S 2 7において、印刷データの出力処理が行われる。S 2 7における出力処理は、ストレージ 2 1～2 3に一時的に印刷データを格納した後、プリンタ 3 1～3 4へ送信されて出力される場合と

、ストレージ 21～23 を介さず直接プリンタ 31～34 において出力が行われる場合とに分けられる。

【0159】

先ず、印刷データがストレージ 21～23 を介さず、直接プリンタ 31～34 に送信されて出力される場合について説明する。

【0160】

この場合には、S33 において、該当するプリントの使用料に応じた課金処理が行われた後、S34 において、印刷データが作成される。そして、上記印刷データは、S35 において、該当するプリンタ 31～34 へ送信され印刷処理が行われる。

【0161】

次に、印刷データが、ストレージ 21～23 に一時的に格納された後、プリンタ 31～34 へ送信されて出力される場合について説明する。

【0162】

この場合は、図 8 (c) に示す表示画面において、「ストレージへ出力」というボタンを選択する。すると、ホスト PC 11～14 の表示部には、図 8 (d) に示すように、S28 において、選択されたプリンタ 31～34 に対して出力可能なストレージ 21～23 を表示する画面が現れる。よって、ユーザは、S29 において、その印刷データに見合ったセキュリティレベルおよび料金を備えたストレージを選択することができる。なお、S29 において、ユーザが希望するストレージが一覧にない場合には、再度、S23 に戻って検索カテゴリーの選択からやり直すこともできる。

【0163】

S29 において、ストレージが選択されると、S30 において、選択されたプリンタおよびストレージの使用料に応じた課金処理が行われた後、印刷データが作成される。そして、印刷データは、S32 において、選択されたストレージへ送信される。

【0164】

本実施形態の印刷システムでは、以上のような方法により、ホスト PC 11～

14からストレージまたはプリンタに対して印刷データの送信が行われることで、ユーザの希望する場所に設置されたプリンタにおいて印刷データを出力できる。さらに、印刷データの重要度に応じて、セキュリティレベルの異なる複数の印刷データの送信ルートから最適なルートを選択することができるため、操作性に優れ、かつ印刷データ保護の観点から安全性の高い印刷システムを実現できる。

【0165】

さらに、本実施形態の印刷システムにおいて、各ストレージが持つ機能を優先してストレージを検索し、印刷データの送信ルートを決定する方法について、図9のフローチャートを用いて説明すれば以下のとおりである。

【0166】

ホストPC11～14から印刷データの送信を開始する場合には、図9に示すように、S41において、最初にホストPC11～14内の検索ドライバ115を起動させ、S42において、該ホストPC11～14を検索サーバ41に接続する。

【0167】

すると、ホストPC11～14の図示しない表示部には、図10（a）に示すような表示画面が現れ、検索カテゴリー（検索条件）を選択することができる。

【0168】

ここで、ストレージのセキュリティレベルを優先して検索を行う場合には、S43において、「ストレージ」ボタンを選択する。

【0169】

続いて、ホストPC11～14の表示部には、図10（b）に示すような表示画面が現れ、ユーザは、S44において、例えば、名前、セキュリティなどのストレージ21～23の検索条件を入力する。なお、図10（b）では、検索条件として、ストレージ21～23の「名前」を選択した場合を示している。

【0170】

ここで、例えば、ストレージSC23が選択されると、S45において、図10（c）に示すような表示画面が現れる。あるいは、S45において、ストレージSA21が選択されると、図10（d）に示すような表示画面が現れる。

【0171】

そして、図10(c)または図10(d)に示す表示画面に表示されたストレージSA21またはストレージSC23に対応する出力可能なプリンタ、ストレージとプリンタとの組合せ(ルート)によって定まるセキュリティレベル、および出力に要する料金が、その印刷データに見合ったものであれば、図10(c)または図10(d)において「OK」ボタンを選択し、S46において、ストレージの選択を行う。

【0172】

ここで、出力可能プリンタ、セキュリティレベルおよび料金等が、ユーザの希望するものでない場合には、再度、S43に戻って、検索カテゴリーの選択からやり直すことができる。

【0173】

S46において、ユーザの希望するストレージが選択されると、S47において、該当するストレージの使用料に応じた課金処理が行われた後、S48において、印刷データが作成される。そして、S49において、上記印刷データは該当するストレージへ送信される。

【0174】

本実施形態の印刷システムは、以上のように、ホストPC11～14からストレージ21～23に対して印刷データが送信されることにより、所望のセキュリティレベルのストレージに対して印刷データの送信し、該印刷データを記憶することができる。さらに、印刷データの重要度に応じて、セキュリティレベルの異なる複数の送信ルートの中から最適なルートを選択することができるため、操作性に優れ、かつデータ保護の観点から安全性の高い印刷システムを実現できる。

【0175】

さらに、本実施形態に係る印刷システムにおいては、プリンタ31～34から、検索サーバ41を用いて所望のセキュリティレベルのストレージを検索し、該検索されたストレージに蓄積された印刷データを取得することもできる。以下に、プリンタ31～34からストレージ21～23を検索する方法について、図11に示すフローチャートを用いて説明する。

【0176】

任意のプリンタから印刷データの検索を開始する場合には、図11に示すように、S61において、最初にプリンタ31～34における図示しない検索ドライバを起動し、S62において、該プリンタを検索サーバ41に接続する。

【0177】

すると、プリンタの表示部には、上段にて説明した図10（a）に示す検索カテゴリーを表示する画面が現れ、検索カテゴリー（検索条件）を選択することができる。

【0178】

ここで、ストレージに応じた検索を行う場合には、S63において、「ストレージ」ボタンを選択する。

【0179】

続いて、プリンタの表示部上には、図10（b）に示す表示画面が現れ、ユーザは、S64において、例えば、名前、セキュリティレベルなどのストレージの検索条件を入力する。すると、S65において、プリンタの表示部にはその検索結果が表示され、S66において、ユーザは目的とする印刷データが格納されているストレージを選択することができる。なお、再度、検索条件の選択をやり直したい場合は、S63に戻ることも可能である。

【0180】

S66において、目的とする印刷データが格納されているストレージを選択すると、S67において、その印刷データが当該プリンタにおいて印刷可能であるか否かについて判断される。すなわち、ここでは、現在ユーザが操作を行っているプリンタに対して、セキュリティの面で、所望の印刷データが格納されたストレージからデータを取得することが可能であるか否かについて判断される。

【0181】

S67で印刷可能と判断された場合、すなわちYesが選択された場合には、S68において、検索したストレージから印刷データを取得できる。そして、S69において印刷が行われた後、S70において、使用料金に応じた課金処理が行われて、処理が終了する。

【0182】

一方、S67において印刷不可能と判断された場合、すなわちNoが選択された場合には、S71において、その旨が表示部によって報知される。そして、S72において、ユーザは、印刷可能なプリンタを再度検索するか否かを選択することができる。S72において、再検索を行うことを選択した場合、すなわちYesを選択した場合には、S73において、印刷可能なプリンタの検索を行うことができる。また、S72において、再検索を行わないことを選択した場合、すなわちNoが選択された場合には、処理を終了する。

【0183】

本実施形態の印刷システムでは、以上のように、プリンタと印刷データが格納されているストレージとのセキュリティレベルが一致せず、かつプリンタのセキュリティレベルがストレージのセキュリティレベルよりも低い場合には、そのストレージからプリンタに対して印刷データを送信することができない。

【0184】

これにより、印刷データが記憶されているストレージよりもセキュリティレベルが低いプリンタから、誤ってセキュリティレベルの高い印刷データを出力する等の問題の発生を防止し、印刷データの安全性を確保できる。

【0185】

また、上記のように、セキュリティレベルの不適合により、必要な印刷データが格納されているストレージからプリンタに対して該印刷データの送信ができない場合には、ユーザが操作しているプリンタの検索部316によって、該ストレージとセキュリティレベルが合致したプリンタを検索することができる。このため、ユーザは、操作中のプリンタ以外に、セキュリティレベルの合致したプリンタをすぐに把握でき、設置場所、機能等の条件が合えば、その新たに検索されたプリンタから印刷データを出力することができる。

【0186】

なお、本実施形態では、ホストPCについてセキュリティレベルは特に設定されていなかったが、本発明はこれに限定されるものではなく、ホストPCについても、ストレージやプリンタと同様に、セキュリティレベルが設定されていても

よい。

【0187】

〔実施形態2〕

本発明の電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法の他の実施形態に係る印刷システムについて、図12～図14(c)を用いて説明すれば以下のとおりである。なお、説明の便宜上、上記実施形態1にて説明した図面と同じ機能を有する部材については、同じ符号を付記し、その説明を省略する。

【0188】

本実施形態の印刷システムは、基本的な構成としては、上記実施形態1におけるネットワークと同様である。しかし、本実施形態におけるネットワークでは、ネットワークの一部が、会社内など狭い範囲内での通信を可能にするイントラネットを介して接続されている点で異なっている。

【0189】

本実施形態の印刷システムが接続されているネットワークにおいては、図12に示すように、ホストHA11、ストレージSA21、プリンタ31が、イントラネット60上でのみ接続可能な機器である。

【0190】

また、ホストHB12、ストレージSB22、プリンタ32は、イントラネット60およびインターネット61の双方から接続可能な機器である。なお、検索サーバ41についても、イントラネット60およびインターネット61の両方のネットワークに接続されているホストPCおよびプリンタから接続することができる。

【0191】

ホストHC13、ホストHD14、プリンタPC33、ストレージSC23およびプリンタPD34は、インターネット61上でのみ接続することができる機器である。

【0192】

なお、図12において斜線で囲まれた領域、すなわちイントラネット60およ

びインターネット 61 の双方から接続可能なネットワーク 62 と、イントラネット 60 上のネットワークとの双方に含まれる各機器は、データ保護（セキュリティ）の観点から、データ保安用のシステムであるルータ（アクセス制御手段）42 を介してイントラネット 60 内の他の機器と接続されている。また、図 12 において斜線で囲まれた領域、すなわちインターネット 61 とイントラネット 60 との双方に含まれるネットワーク 62 に配置された機器は、同じくデータ保護（セキュリティ）の観点から、データ保安用のシステムである firewall（アクセス制御手段）43 を介して、インターネット 61 内の他の機器と接続されている。

【0193】

ホスト PC 11～14 のホスト情報記憶部 113 には、図 13（a）に示すように、各ホスト PC 11～14 の接続可能なストレージおよびその設置場所が記憶されている。この接続可能なストレージについては、図 12 に示すネットワークの構成により決定される。例えば、ホスト HC 13 については、イントラネット 60 内のストレージ SB 22 とも接続できるようになっている。

【0194】

プリンタ 31～34 のプリンタ情報記憶部 313 には、図 13（b）に示すように、各プリンタ 31～34 の接続可能ストレージが記憶されている。この接続可能ストレージについては、上記と同様に、図 12 に示すネットワーク構成により決定される。例えば、プリンタ PC 33 については、ストレージ SB 22 とも接続できるようになっている。また、プリンタ情報記憶部 313 には、各プリンタの設置場所、および、各プリンタが備えているカラー、両面、ステープルなどの印刷機能に関する情報も記憶されている。この記憶情報については、各プリンタの図示しない表示部、あるいは検索サーバ 41 を介して、各ホスト PC から確認することができる。

【0195】

ストレージ 21～23 のストレージ情報記憶部 213 には、図 13（c）に示すように、各ストレージ 21～23 の接続可能ホスト、接続可能プリンタ、設置場所が記憶されている。上記接続可能ホスト、および上記接続可能プリンタについては、図 12 に示すネットワーク構成に示す通りであるが、ストレージ S b 2

2については、インターネット61上のホストHC13およびプリンタPC33と接続できるようになっている。

【0196】

検索サーバ41の機器情報記憶部413には、図13(d)に示すように、各ストレージSA～SCが接続可能なホストHA～HDおよびプリンタPA～PDが記憶されているとともに、各ホスト、各ストレージを介して各プリンタにおいて印刷処理を行った場合のセキュリティレベルが記憶されている。

【0197】

本実施形態の印刷システムでは、このような機器情報記憶部413を備えた検索サーバ41を備えることによって、各印刷データの重要度に応じてセキュリティレベルを設定し、そのセキュリティレベルに対応する各種機器（ストレージ、プリンタ）を選択して処理を行うことができる。

このように、本実施形態の印刷システムでは、図13(d)に示すように、その印刷データのセキュリティレベルが異なる3つの印刷ルート（すなわち、ストレージ、ホスト、プリンタの組合せ）が存在する。

【0198】

なお、セキュリティレベル「高」とは、ネットワーク的にも、物理的にもデータ保護の観点からも高い安全性を有するものを意味している。本実施形態の印刷システムにおけるセキュリティレベル「高」の印刷ルートとしては、例えば、会社内のイントラネット60上にある機器のみを経由するルートがある。

【0199】

また、セキュリティレベル「中」とは、ネットワーク的な面では安全性に問題があるが、物理的には高い安全性を有するものを意味している。本実施形態の印刷システムにおけるセキュリティレベル「中」の印刷ルートとしては、例えば、会社内に設置されているホストおよびプリンタを用いているが、社外のインターネット61上にあるホスト、プリンタ、ストレージとも接続できる印刷ルートがある。

【0200】

さらに、セキュリティレベル「低」とは、ネットワーク的な面からも、物理的

な面からもデータ保護の観点から危険性を有するもののことを意味している。本実施形態の印刷システムにおいて、セキュリティレベル「低」の印刷ルートとしては、例えば、インターネット 61 上で誰でもアクセスすることが可能な機器を経由するルートがある。

【0201】

なお、本実施形態の印刷システムが備えている検索サーバ 41 には、図 14 (a) ～図 14 (c) に示すように、各セキュリティレベルに応じて、ストレージとプリンタとを組み合わせる構成される印刷ルートを検索する図示しないルート検索部（ルート検索手段）が設けられていてもよい。

【0202】

例えば、所望のセキュリティレベルが「高」以上の場合には、図 14 (a) に示すように、ホスト HA11 またはホスト HB12 を選択し、ストレージ SA21 を選択し、プリンタ PA31 またはプリンタ 32 PB を選択する印刷ルートが検索される。

【0203】

また、所望のセキュリティレベルが「中」の場合には、図 14 (b) に示すように、ホスト HA11、ホスト HB12、ホスト HC13 の何れかのホスト PC と、ストレージ SB22 と、プリンタ PA31、プリンタ PB32、プリンタ PC33 の何れかのプリンタとを選択する印刷ルートが検索される。

【0204】

また、所望のセキュリティレベルが「低」の場合には、図 14 (c) に示すように、ホスト HB12、ホスト HC13、ホスト HD14 の何れかのホスト PC と、ストレージ SC23 と、プリンタ PC33、プリンタ PD34 の何れかのプリンタとを選択する印刷ルートが検索される。

【0205】

本実施形態の印刷システムは、以上のように、検索機能を備えているため、所望のセキュリティレベルに応じた印刷ルートを容易に検索することができ、効率よく印刷ルートを選択できる。

【0206】

なお、本実施形態の印刷システムにおいて実行されるセキュリティレベルに応じた印刷データの送信については、上述の実施形態 1 に記載の方法と同様にして実行することができるため、説明を省略する。

【0207】

〔実施形態 3〕

本実施形態の電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法のさらに他の実施形態に係るスキャナシステムについて、図 15～図 18 を用いて説明すれば以下のとおりである。なお、説明の便宜上、上記実施形態 1 にて説明した図面と同じ機能を有する部材については、同じ符号を付記し、その説明を省略する。

【0208】

本実施形態のスキャナシステムは、図 1 に示すホスト PC（外部機器） 11～14、ストレージ 21～23、プリンタ 31～34 および検索サーバ（検索手段） 41 に加えて、図 15 に示すような、スキャナ（電子機器） 51～54 を備えている。そして、スキャナ 51～54 からスキャンデータをホスト PC に対してデータを送信する点で、ホスト PC 11～14 からプリンタ 31～34 に対して印刷データを送信する上記実施形態 1・2 と異なっている。

【0209】

スキャナ 51～54 は、通信部 511、制御部 512、スキャナ情報記憶部 513、暗号化部 514、検索部 515、操作部 516 および画像読取部 517 を備えている。

【0210】

通信部 511 は、外部の各機器とのデータの送受信を行うインターフェース部である。

【0211】

制御部 512 は、スキャナ装置全体を制御する装置の中心となる部分である。

【0212】

スキャナ情報記憶部 513 は、スキャナ装置の設置場所、機能、セキュリティレベルなどのスキャナ装置に関する情報を記憶している。なお、ここに記憶され

ている情報についても、図示しない表示手段によって表示され、ユーザが確認することができる。

【0213】

暗号化部 514 は、スキャンデータを保護するために、スキャンデータの内容が第三者によって容易に読み取られないように、スキャンデータの暗号化処理を行う。

【0214】

検索部 515 は、セキュリティレベル等に応じて、ネットワークに接続されているストレージやプリンタの検索を行う。

【0215】

操作部 516 は、ユーザが直接スキャナ装置を操作する際に使用され、ユーザからの指示を入力する。

【0216】

画像読取部 517 は、スキャナ機能によって原稿を読み取り、画像データとして取り込む。

【0217】

各ストレージ 21～23、各プリンタ 31～34、各ホスト PC 11～14、検索サーバ 41 における各情報記憶部 113・213・313・413 は、図 16 (a)～図 16 (d) に示すように、各種情報を記憶している。

【0218】

各ストレージ 21～23 におけるストレージ情報記憶部 213 は、図 16 (a) に示すように、ストレージ名、ストレージ使用料金およびセキュリティレベルを示すデータ保護機能を記憶している。

【0219】

例えば、ストレージ SA 21 は、セキュリティレベルが「高」であり、スキャンデータを暗号化して送信することができる暗号化プロトコル 2.0 という暗号化保護機能を備えている。

【0220】

ストレージ SB 22 は、セキュリティレベルが「中」であり、スキャンデータ

を暗号化して送信することができる暗号化プロトコル 1. 0 を備えている。

【0221】

ストレージサーバ SC23 は、セキュリティレベルが「低」であって、データ保護目的の機能を特に備えていない。

【0222】

本実施形態のスキャンシステムでは、実施形態 1 の図 3 と同様に、データ保護に関するセキュリティレベルの異なる 3 つのストレージを備えている。

【0223】

次に、各スキャナ 51～54 におけるスキャナ情報記憶部 513 は、図 16 (b) に示すように、スキャナ名、セキュリティレベルを示すデータ保護機能、スキャナの設置場所、および各スキャナが備えているスキャナ機能について記憶している。

【0224】

スキャナ ScA51 は、暗号化プロトコル 2. 0 および 1. 0、暗号化機能を備えており、セキュリティレベルは「特高」である。

【0225】

スキャナ ScB52 は、暗号化プロトコル 2. 0 および 1. 0 を備えており、セキュリティレベルは「高」である。

【0226】

スキャナ ScC53 は、暗号化プロトコル 1. 0 のみを備えており、セキュリティレベルは「中」である。

【0227】

スキャナ ScD54 は、データ保護目的の機能を特に備えておらず、セキュリティレベルは「低」である。

【0228】

また、スキャナ情報記憶部 513 は、各スキャナの設置場所および各スキャナが備えているカラー、モノクロおよび解像度等のスキャナ機能に関する情報についても記憶している。この記憶情報については、各スキャナの図示しない表示部、あるいは検索サーバ 41 を介して、各ホスト PC から確認することができる。

【0229】

各ホストPC11～14のホスト情報記憶部113は、図16（c）に示すように、ホスト名と、各ホストPC11～14のセキュリティレベルを示すデータ保護機能と、データ暗号復号機能の有無に関する情報とを記憶している。

【0230】

本実施形態の各ホストPC11～14は、スキャンデータを暗号化して送信することができる暗号化プロトコル2.0および1.0を備えており、暗号化プロトコルを備えていないホストHD14を含めて、セキュリティレベル「低」から「高」までの全てのレベルに対応可能である。

【0231】

検索サーバ41の機器情報記憶部413は、図16（d）に示すように、ルート、暗号化プロトコルの有無、データ暗号化の有無、およびセキュリティレベルに関する情報を記憶している。

【0232】

これらの情報は、検索サーバ41が、各スキャナ51～54からスキャナ情報、各ストレージ21～23からストレージ情報、各ホストPC11～14からホスト情報をそれぞれ収集することにより取得してもよいし、予め作成された情報を記憶しておいてもよい。

【0233】

本実施形態のスキャナシステムにおいては、検索サーバ41がこのような機器情報記憶部413を備えていることにより、各スキャナ51～54から、各スキャンデータに対して付与すべきセキュリティレベルに応じて、各機器（ストレージ21～23、ホストPC11～14）を選択することができる。

【0234】

なお、検索サーバ41には、図17（a）～図17（f）に示すように、各セキュリティレベルに応じて、スキャナとストレージとホストPCとを組み合わせたデータの送信ルートを検索する図示しないルート検索部（ルート検索手段）が設けられていてもよい。

【0235】

例えば、ユーザ所望のセキュリティレベルが「特高」である場合には、検索サーバ41は、図17(a)に示すように、スキャナScA51と、ストレージSA21と、ホストHA11とを組み合わせたデータの送信ルートであって、かつ暗号化した状態でデータを送信するルートを検索することができる。

【0236】

具体的には、スキャナにおいて、スキャンデータの暗号化を行い、ストレージにおいてスキャンデータの暗号化はそのまま、暗号化プロトコル2.0を用いて送信し、ホストPCにおいてデータ利用時に復号化すればよい。

【0237】

また、ユーザ所望のセキュリティレベルが「高」である場合には、検索サーバ41は、図17(b)に示すように、スキャナScA51あるいはスキャナScB52と、ストレージSA21と、ホストHA11あるいはホストHB12とを組み合わせたデータの送信ルートを検索することができる。

【0238】

具体的には、スキャナからデータを暗号化プロトコル2.0で送信し、ストレージにおいて保存し、データ利用時には、ストレージにおいてデータを復号化し、暗号化プロトコル2.0でホストPCへ送信すればよい。

【0239】

また、ユーザ所望のセキュリティレベルが同じく「高」である場合には、検索サーバ41は、図17(c)に示すように、スキャナScA51と、ストレージSB22と、ホストHA11あるいはホストHC13とを組み合わせたデータの送信ルートであって、かつ暗号化した状態でデータを送信するルートを検索することができる。

【0240】

具体的には、スキャナにおいてスキャンデータの暗号化を行い、暗号化プロトコル1.0でデータを送信し、暗号化されたままストレージにおいて保存し、データ利用時には、暗号化プロトコル1.0でデータを送信し、ホストPCにおいて復号化すればよい。

【0241】

さらに、ユーザ所望のセキュリティレベルが「中」である場合には、検索サーバ41は、図17(d)に示すように、スキャナScA51あるいはスキャナScB52あるいはスキャナScC54と、ストレージSB22と、ホストHA11あるいはホストHB12あるいはホストHC13とを組み合わせたデータの送信ルートを検索することができる。

【0242】

具体的には、スキャナにおいてスキャンデータを暗号化プロトコル1.0で送信し、ストレージにおいて保存し、データ利用時には、暗号化プロトコル1.0でスキャンデータを送信すればよい。

【0243】

また、ユーザ所望のセキュリティレベルが同じく「中」である場合には、検索サーバ41は、図17(e)に示すように、スキャナScA51と、ストレージSB23と、ホストHA11あるいはホストHC13とを組み合わせたデータの送信ルートであって、かつ暗号化した状態でデータを送信するルートを検索することができる。

【0244】

具体的には、スキャナにおいてスキャンデータを暗号化し、ノンセキュリティ通信で送信し、ストレージにおいて暗号化されたデータをそのまま保存し、暗号化されたデータをノンセキュリティ通信して、データ利用時に復号化すればよい。

【0245】

ユーザ所望のセキュリティレベルが「低」の場合には、検索サーバ41は、図17(f)に示すように、スキャナScA51～ScD54の何れかのスキャナと、ストレージSC23と、ホストHA11～HD14の何れかのホストPCとを組み合わせたデータの送信ルートを検索することができる。

【0246】

具体的には、スキャンデータをそのままノンセキュリティ通信で送信し、スキャンデータをそのまま保存し、ホストPCへのノンセキュリティ通信でスキャンデータを送信すればよい。

【0247】

本実施形態のスキャナシステムは、このように、セキュリティレベルに応じて、データの送信ルートを容易に検索することができるため、データ保護のセキュリティ面を考慮して、スキャナからホストPCまでデータを送信することができる。

【0248】

スキャナ51～54において、スキャンデータの送信を開始する場合には、図18に示すように、S81において、最初にスキャナ51～54の検索部515を起動する。これにより、S82において、該スキャナ51～54と検索サーバ41とが接続される。

【0249】

ここで、セキュリティレベルに応じた検索を行う場合には、S83において、「セキュリティ」ボタンを選択する。

【0250】

S84において、例えば、セキュリティレベル「高」が選択されると、S85において、目的とするセキュリティレベルに応じたストレージが表示される。

【0251】

そして、S86において、ユーザは3つのストレージから任意のストレージを選択する。

【0252】

S86において、ユーザが所望のストレージを選択すると、S87において、先に選択したストレージとセキュリティレベルとに応じて、接続可能なホストPCが表示される。

【0253】

ここで、表示された接続可能なホストPCの設置場所あるいは機能がユーザの希望に合致するものでない場合、すなわち、S88においてYesの場合には、再度S83より操作をやり直すことができる。

【0254】

一方、上記接続可能ホストPCの機能、セキュリティレベル等が、ユーザの希

望に合致するものである場合、すなわち、S88においてNoの場合には、S89において、ストレージ使用料として課金処理が行われた後、S90において、スキャンが開始される。そして、暗号化プロトコルを利用してスキャンデータの暗号化処理がされた後、S91において、該当するストレージへの送信が行われる。

【0255】

本実施形態のスキャナシステムでは、以上のように、スキャナからストレージに対してスキャンデータが送信されるため、スキャンデータのセキュリティレベルに応じたルートでスキャンデータの送信処理を行うことができ、データ保護の観点から安全性の高いスキャナシステムを実現できる。

【0256】

また、上記実施形態1・2のように、ホストPCからストレージ、プリンタに対してデータを送信してもよいし、本実施形態のように、スキャナ装置等の電子機器からストレージ、ホストPC、その他の外部機器等へデータを送信してもよい。

【0257】

さらに、図17(a)、図17(c)および図17(e)に示すように、スキャナ、ストレージ、ホストPCのそれぞれが有している暗号化プロトコル等の通信データ保護機能と、データの暗号化とを組み合わせることにより、ユーザが選択可能なデータ送信ルートの選択肢を増やすことができる。

【0258】

なお、上述した実施形態1～3において説明した電子機器ネットワークシステムは、本発明の一例であって、本発明は上記各実施形態の記載に限定されるものではない。例えば、より多くのホストPC、ストレージ、プリンタを備えた印刷システムに対しても適用可能である。さらに、印刷システム以外にも、実施形態3で説明したスキャナ等のようなプリンタ以外の電子機器を用いてネットワークを構成した電子機器ネットワークシステムであってもよい。

【0259】

また、上記各実施形態1～3では、電子機器（ホストPC、スキャナ）、外部

機器（プリンタ、ホストPC）および記憶手段（ストレージ）のそれぞれについてセキュリティレベルを付与した例をあげて説明したが、本発明はこれに限定されるものではない。例えば、ユーザにもセキュリティレベルが設定されており、上記実施形態1～3で説明した電子機器、外部機器および記憶手段等と組み合わせてもよい。これにより、機密性の高いデータについては、特定のユーザに限ってセキュリティレベルが「特高」の機器を利用できるようにすれば、さらに安全性が高い電子機器ネットワークシステムを構築できる。

【0260】

本発明は上述した各実施形態に限定されるものではなく、請求項に示した範囲で種々の変更が可能であり、異なる実施形態にそれぞれ開示された技術的手段を適宜組み合わせて得られる実施形態についても本発明の技術的範囲に含まれる。

【0261】

本発明は、ホストPCから送られた印刷データを記憶する複数のストレージと、上記ストレージから該印刷データを取得し印刷を行う複数のプリンタとを備えた印刷システムにおいて、上記複数のストレージは、ストレージごとにセキュリティレベルが異なり、上記印刷システムは、ユーザにとって指定された上記印刷データのセキュリティレベルに応じて、当該印刷データが格納されるストレージを検索する検索手段をさらに備えることを特徴とする電子機器ネットワークシステムと表現することもできる。

【0262】

本発明は、ホストPCから送られた印刷データを記憶する複数のストレージと、上記ストレージから該印刷データを取得し印刷を行う複数のプリンタとを備えた印刷システムにおいて、ユーザによって指定された上記印刷データのセキュリティレベルに応じて、当該印刷データが格納されるストレージを検索する第1の検索手段と、上記検索手段の検索結果によって選択されたストレージのセキュリティレベルを示す表示手段と、当該ストレージから印刷データを取得し印刷可能なプリンタを検索する第2の検索手段とをさらに備えることを特徴とする印刷システムと表現することもできる。

【0263】

【発明の効果】

本発明の電子機器ネットワークシステムは、以上のように、電子機器、記憶手段および外部機器は、それぞれがセキュリティ機能を有している構成である。

【0264】

それゆえ、電子機器から記憶手段を介して外部機器へデータを送信する場合には、ユーザが希望するセキュリティレベルに対応するセキュリティ機能を有する記憶手段および外部機器を選択することで、データを安全かつ容易に記憶手段および外部機器に対して送信できるという効果を奏する。

【0265】

よって、ユーザは、重要なデータを安全に送信したい場合には、IDやパスワードを入力することなく、単に、所望のセキュリティレベルに合致した記憶手段および外部機器を選択するだけで、データの安全性を確保した電子機器ネットワークシステムを実現することが可能となる。

【0266】

上記電子機器、記憶手段および外部機器が有しているセキュリティ機能のセキュリティレベルに応じて、上記電子機器、記憶手段および外部機器を検索する検索手段を備えていることがより好ましい。

【0267】

それゆえ、ユーザは送信するデータの重要度に応じて、セキュリティレベルを設定するだけで、ネットワークに接続された複数の記憶手段、外部機器の中から、設定されたセキュリティレベルに対応する記憶手段および外部機器を容易に検索することができる。よって、ユーザは、所望のセキュリティレベルのセキュリティ機能を有する記憶手段と外部機器とを組み合わせたルートに沿って、データを安全に送信することができるという効果を奏する。

【0268】

上記外部機器の設置場所または外部機器が備えている機能に基づいて、上記外部機器の検索を行う検索手段を備えていることがより好ましい。

【0269】

それゆえ、ユーザは、データを出力する外部機器が設置されている場所や外部

機器が備えている機能に基づいて外部機器を検索することができるため、ネットワークに接続された複数の外部機器の中から、ユーザの希望に沿った外部機器をより容易に選択することができるという効果を奏する。

【0270】

また、送信されるデータの処理が特殊である場合には、外部機器の機能に基づいてその処理を行う機能を備えた外部機器を検索することができ、より詳細な検索が可能になる。

【0271】

上記検索手段は、上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することがより好ましい。

【0272】

それゆえ、ユーザは、所望のセキュリティレベルあるいは外部機器の設置場所、機能等に基づいて、電子機器から記憶手段を介して外部機器に至るまでのデータの送信ルートを検索することができるという効果を奏する。よって、ユーザ所望のセキュリティレベルに応じて別々に検索した記憶手段および外部機器を組み合わせる送信ルートを決する場合と比較して、効率よく所望のセキュリティレベルに適合する送信ルートを見つけることができる。

【0273】

上記外部機器は、自機のセキュリティレベルに対応する記憶手段を検索する検索部を備えていることがより好ましい。

【0274】

それゆえ、ユーザが操作している外部機器においても、その外部機器に対してデータの送信が可能なセキュリティ機能を有する記憶手段を検索することができるため、ユーザは外部機器において、直接データが格納されている記憶手段から必要なデータを取得することが可能になるという効果を奏する。よって、外部機器において、記憶手段からデータを取得する場合でも、データの安全性を考慮した出力が可能になる。また、ユーザが操作中の外部機器に対してデータを送信することができる記憶手段を検索することで、セキュリティレベルが合わないため、記憶手段に格納されたデータを目的とする外部機器から取り出すことができな

いといった問題を未然に防止することができる。

【0275】

上記電子機器は、上記検索手段による検索条件を入力し、該検索結果を表示する表示手段を備えていることがより好ましい。

【0276】

それゆえ、ユーザは検索条件を容易に入力できるとともに、検索結果としてセキュリティレベル、ストレージの使用料金、外部機器の設置場所、外部機器の機能等を表示することができ、ユーザの操作性を向上することができるという効果を奏する。

【0277】

上記電子機器、記憶手段および外部機器のセキュリティ機能は、アクセス制御手段を介して接続された複数のネットワークのうち、どのネットワークに配置されているかによって付与されることがより好ましい。

【0278】

それゆえ、例えば、ルータ、ファイアウォール等のアクセス制御手段を介して接続された企業内のイントラネットと外部の誰からもアクセスが可能なインターネットとを組み合わせることで、上記企業の社員から見て、3段階のセキュリティレベルを設定することができる。よって、ユーザは、重要なデータについては、社内のイントラネットのみに接続可能な機器を用いて印刷データを送信、出力することで、インターネットにしか接続できない外部の機器に対してデータが漏洩することを防止し、安全かつ確実にデータを出力することができるという効果を奏する。

【0279】

上記外部機器は、画像形成装置であることがより好ましい。

【0280】

それゆえ、ホストPC等の電子機器から送信された印刷データを、ネットワークに接続された複数の記憶手段、外部機器の中から、ユーザ所望のセキュリティレベルに適合した記憶手段、画像形成装置に対して送信することができるため、データの安全性を確保した印刷システムを構築できるという効果を奏する。

【0281】

上記電子機器は、スキャナ装置であることがより好ましい。

【0282】

それゆえ、スキャナ装置で読み取った画像データ等を、記憶手段、外部機器あるいは他の電子機器に対して安全に送信することが可能なスキャナシステムを構築できるという効果を奏する。

【0283】

本発明の電子機器ネットワークシステムによるデータ送信先検索方法は、以上のように、上記電子機器、記憶手段および外部機器は、それぞれセキュリティ機能を有しており、上記電子機器からデータを送信する場合には、ユーザが設定したセキュリティレベルに応じて、該セキュリティレベルに適合するセキュリティ機能を備えた上記記憶手段および外部機器の検索を行う構成である。

【0284】

それゆえ、ネットワークを介して複数の電子機器、記憶手段および外部機器がそれぞれ分散配置されたBMLinkS等に適合した電子機器ネットワークシステムにおいて、ユーザが希望するセキュリティレベルに応じて、適合する記憶手段および外部機器を検索できるため、ネットワークに接続された多数の記憶手段および外部機器の中から、安全にデータを送信できる記憶手段および外部機器を容易に見つけることができるという効果を奏する。

【0285】

よって、ユーザは、重要なデータを安全に送信したい場合には、IDやパスワードを入力することなく、単に、所望のセキュリティレベルに合致した記憶手段および外部機器を選択するだけで、データの安全性を確保した電子機器ネットワークシステムを実現することが可能となる。

【0286】

上記外部機器の検索は、外部機器の設置場所、機能に基づいて行われることがより好ましい。

【0287】

それゆえ、ユーザは、データを出力する外部機器が設置されている場所や外部

機器が備えている機能に基づいて外部機器を検索することができるため、ネットワークに接続された複数の外部機器の中から、ユーザの希望に沿った外部機器をより容易に選択することができるという効果を奏する。

【0288】

また、送信されるデータの処理が特殊である場合には、外部機器の機能に基づいてその処理を行う機能を備えた外部機器を検索することができ、より詳細な検索が可能になる。

【0289】

上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することがより好ましい。

【0290】

それゆえ、ユーザは、所望のセキュリティレベル、外部機器の設置場所、機能等に基づいて、電子機器から記憶手段を介して外部機器に至るまでのデータの送信ルートを検索することができるという効果を奏する。よって、ユーザ所望のセキュリティレベルに応じて別々に検索した記憶手段および外部機器を組み合わせで送信ルートを決する場合と比較して、効率よく所望のセキュリティレベルに適合する送信ルートを見つけることができる。

【0291】

セキュリティレベルが合致しない上記電子機器、上記記憶手段および上記外部機器に対するデータの送信を禁止することがより好ましい。

【0292】

それゆえ、ユーザが安全性を重視してデータ送信を行いたい場合でも、誤って誰でもアクセス可能な記憶手段や、誰でも利用可能な外部機器にデータが送信されることを防止でき、より確実にセキュリティ機能を持った所望の外部機器に対してデータを送信できるという効果を奏する。

【0293】

上記外部機器から上記記憶手段に格納されたデータを取り出す際に、必要なデータが格納されている記憶手段とセキュリティレベルが合致せずに該外部機器に対してデータを送信できない場合には、上記検索手段が、上記必要なデータが格

納されている記憶手段とセキュリティレベルが適合する外部機器を検索することがより好ましい。

【0294】

それゆえ、ユーザがある外部機器から、記憶手段に格納されているデータを取り出して出力する場合であって、必要なデータが格納されている記憶手段とセキュリティレベルが合致しない場合には、検索手段が該外部機器に対して出力可能な外部機器を検索することができるという効果を奏する。よって、ユーザは常に必要なデータを取り出せる外部機器を把握して、必要なデータをセキュリティレベルの合致した外部機器から出力することができる。

【図面の簡単な説明】

【図1】

本発明の一実施形態に係る印刷システムが備えているホストPC、ストレージ、プリンタおよび検索サーバの構成を示すブロック図である。

【図2】

図1の印刷システムの概略的な構成を示すブロック図である。

【図3】

(a)～(d)は、各機器における情報記憶部に記憶された記憶内容を示す図である。

【図4】

(a)～(c)は、セキュリティレベル別のデータの送信ルートを示すブロック図である。

【図5】

図1の印刷システムによる、セキュリティレベルを優先して検索した場合の印刷データの送信ルートを検索する手順を示すフローチャートである。

【図6】

(a)～(d)は、図5のフローチャートに示す方法によって印刷データの出力処理を行う場合における、ホストPCに表示される操作画面を示す図である。

【図7】

図1の印刷システムによる、プリンタを優先して検索した場合の印刷データの

送信ルートを検索する手順を示すフローチャートである。

【図 8】

(a) ～ (d) は、図 7 のフローチャートに示す方法によって印刷データの出力処理を行う場合における、ホスト P C に表示される操作画面を示す図である。

【図 9】

図 1 の印刷システムによる、ストレージを優先して検索した場合の印刷データの送信ルートを検索する手順を示すフローチャートである。

【図 10】

(a) ～ (d) は、図 9 のフローチャートに示す方法によって印刷データの出力処理を行う場合に、ホスト P C 上に表示される操作画面を示す図である。

【図 11】

図 1 の印刷システムにおけるプリンタからストレージを検索して印刷データを得る場合の印刷データの送信ルートを検索する手順を示すフローチャートである。

【図 12】

本発明の他の本実施形態に係る印刷システムが構築されているネットワークの構成を示すブロック図である。

【図 13】

(a) ～ (d) は、各機器がそれぞれ備えている各情報記憶部が記憶している記憶内容を示す図である。

【図 14】

(a) ～ (c) は、セキュリティレベルに応じた印刷データの送信ルートを示すブロック図である。

【図 15】

本発明のさらに他の実施形態に係るスキャナシステムのスキャナの内部構成を示すブロック図である。

【図 16】

(a) ～ (d) は、各機器がそれぞれ備えている各情報記憶部が記憶している記憶内容を示す図である。

【図 17】

(a) ～ (f) は、セキュリティレベルに応じた印刷データの送信ルートを示すブロック図である。

【図 18】

図 15 のスキャナシステムにおけるスキャナからホスト P C へデータを送信する場合の送信ルートを検索する手順を示すフローチャートである。

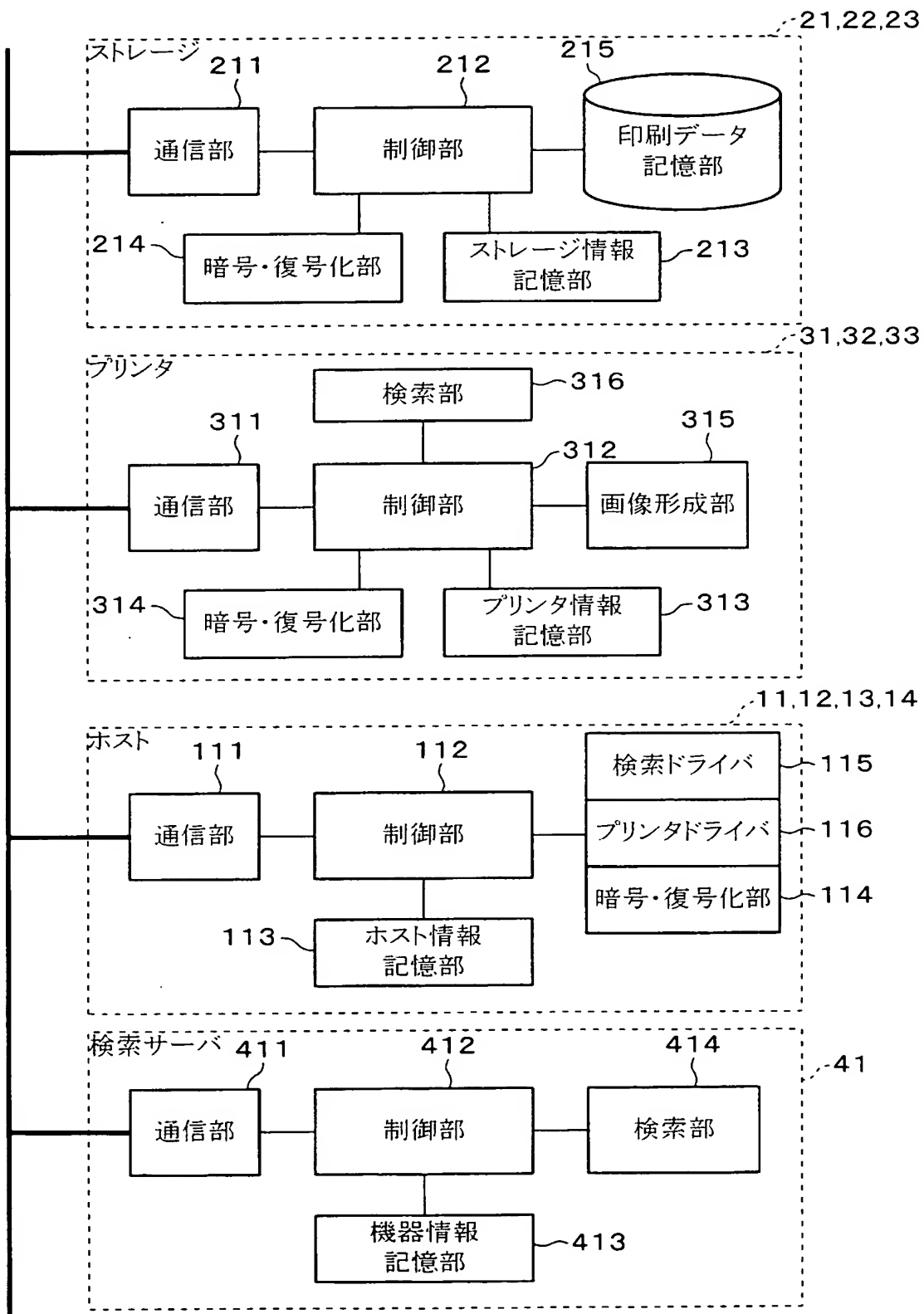
【符号の説明】

1 1 ～ 1 4	ホスト P C (電子機器、外部機器)
2 1 ～ 2 3	ストレージ (記憶手段)
3 1 ～ 3 4	プリンタ (外部機器)
4 1	検索サーバ (検索手段)
4 2	ルータ (アクセス制御手段)
4 3	firewall (アクセス制御手段)
5 1 ～ 5 4	スキャナ (電子機器、外部機器)
6 0	イントラネット
6 1	インターネット
6 2	双方から接続可能なネットワーク
1 1 1	通信部
1 1 2	制御部
1 1 3	ホスト情報記憶部
1 1 4	暗号・復号化部
1 1 5	検索ドライバ
1 1 6	プリンタドライバ
2 1 1	通信部
2 1 2	制御部
2 1 3	ストレージ情報記憶部
2 1 4	暗号・復号化部
2 1 5	印刷データ記憶部
3 1 1	通信部

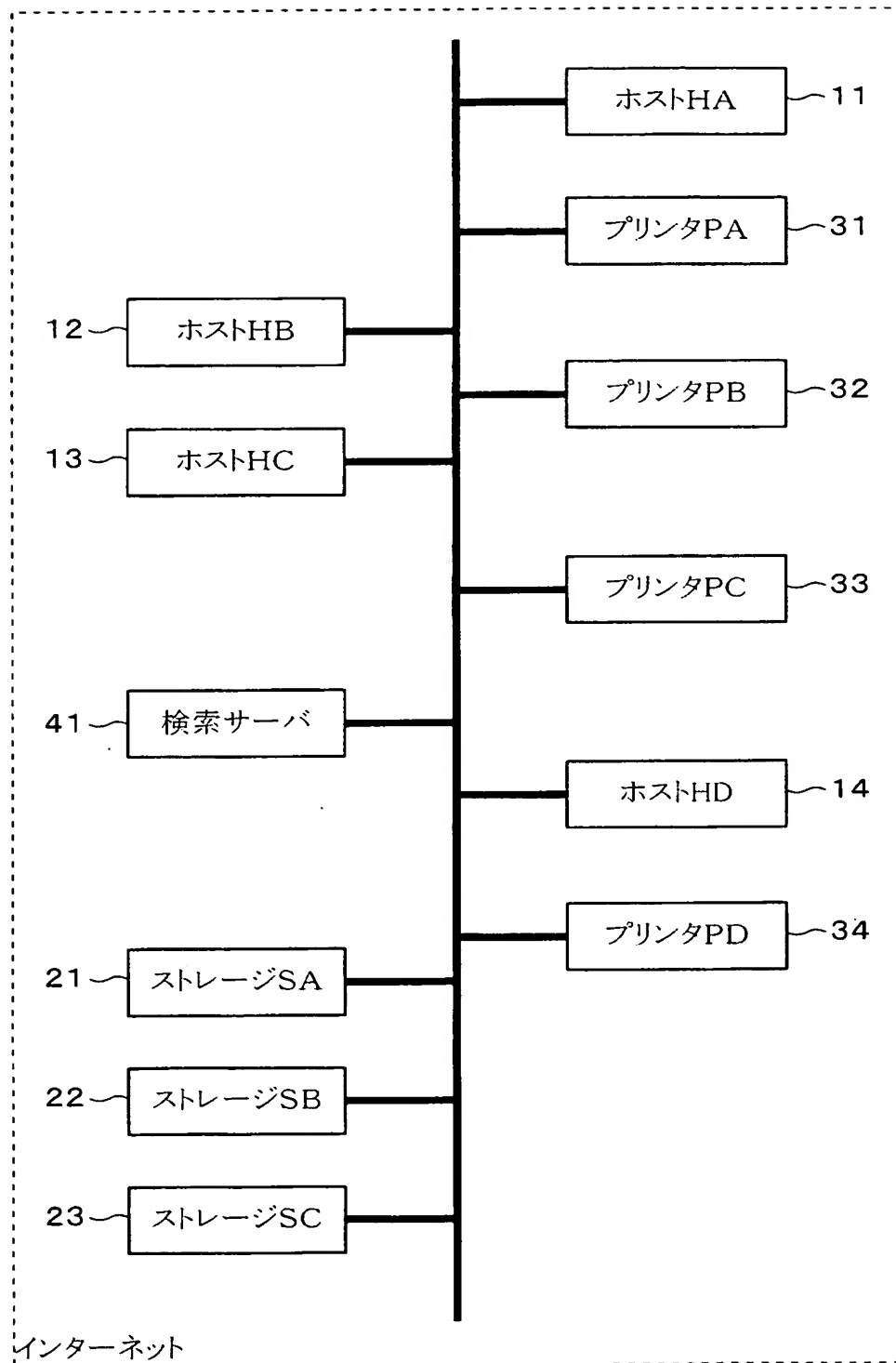
3 1 2	制御部
3 1 3	プリンタ情報記憶部
3 1 4	暗号・復号化部
3 1 5	画像形成部
3 1 6	検索部
4 1 1	通信部
4 1 2	制御部
4 1 3	機器情報記憶部
4 1 4	検索部
5 1 1	通信部
5 1 2	制御部
5 1 3	スキャナ情報記憶部
5 1 4	暗号化部
5 1 5	検索部
5 1 6	操作部
5 1 7	画像読み取り部

【書類名】 図面

【図 1】



【図 2】



【図 3】

(a) ストレージ情報記憶部

ストレージ名	ストレージ 使用料金	データ保護機能 (レベル)	
ストレージ SA	200 円	暗号化プロトコル 2.0 のみ 暗号化保存、バックアップ機能	高 (特高)
ストレージ SB	100 円	暗号化プロトコル 1.0 のみ	中
ストレージ SC	無料	—	低

(b) プリンタ情報記憶部

プリンタ名	データ保護機能 (レベル)		場所	印刷機能
プリンタ PA	暗号化プロトコル 2.0 暗号化プロトコル 1.0 復号化機能	特高	〇〇コンビニ 奈良店	カラー、両面
プリンタ PB	暗号化プロトコル 2.0 暗号化プロトコル 1.0	高	〇〇コンビニ 天理店	両面、ステープル
プリンタ PC	暗号化プロトコル 1.0	中	〇〇コンビニ 郡山店	カラー、両面 ステープル
プリンタ PD	—	低	〇〇コンビニ 高田店	両面、ステープル

(c) ホスト情報記憶部

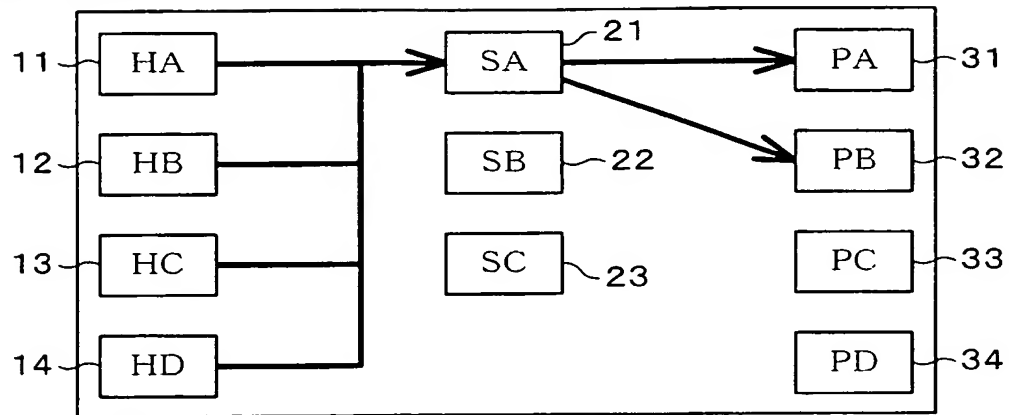
ホスト名	データ保護機能
ホスト HA	暗号化プロトコル 2.0 暗号化プロトコル 1.0
ホスト HB	暗号化プロトコル 2.0 暗号化プロトコル 1.0
ホスト HC	暗号化プロトコル 2.0 暗号化プロトコル 1.0
ホスト HD	暗号化プロトコル 2.0 暗号化プロトコル 1.0

(d) 機器情報記憶部

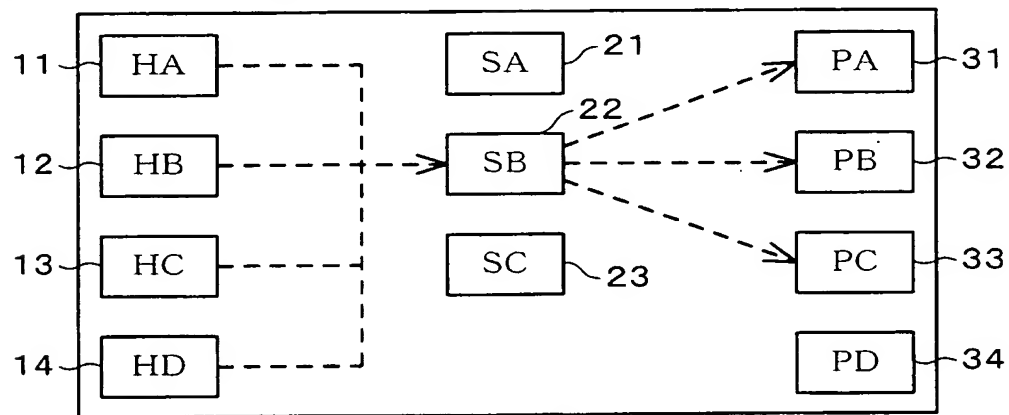
ストレージ名	接続(出力)可能 プリンタ	セキュリティ レベル
ストレージ SA	PA	特高
ストレージ SA	PB	高
ストレージ SB	PA、PB、PC	中
ストレージ SC	PA、PB、PC、PD	低

【図 4】

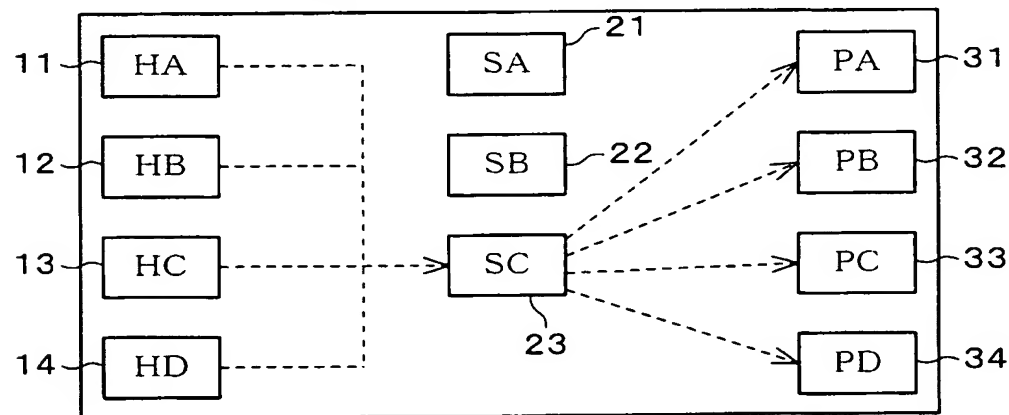
(a) セキュリティレベル: 高



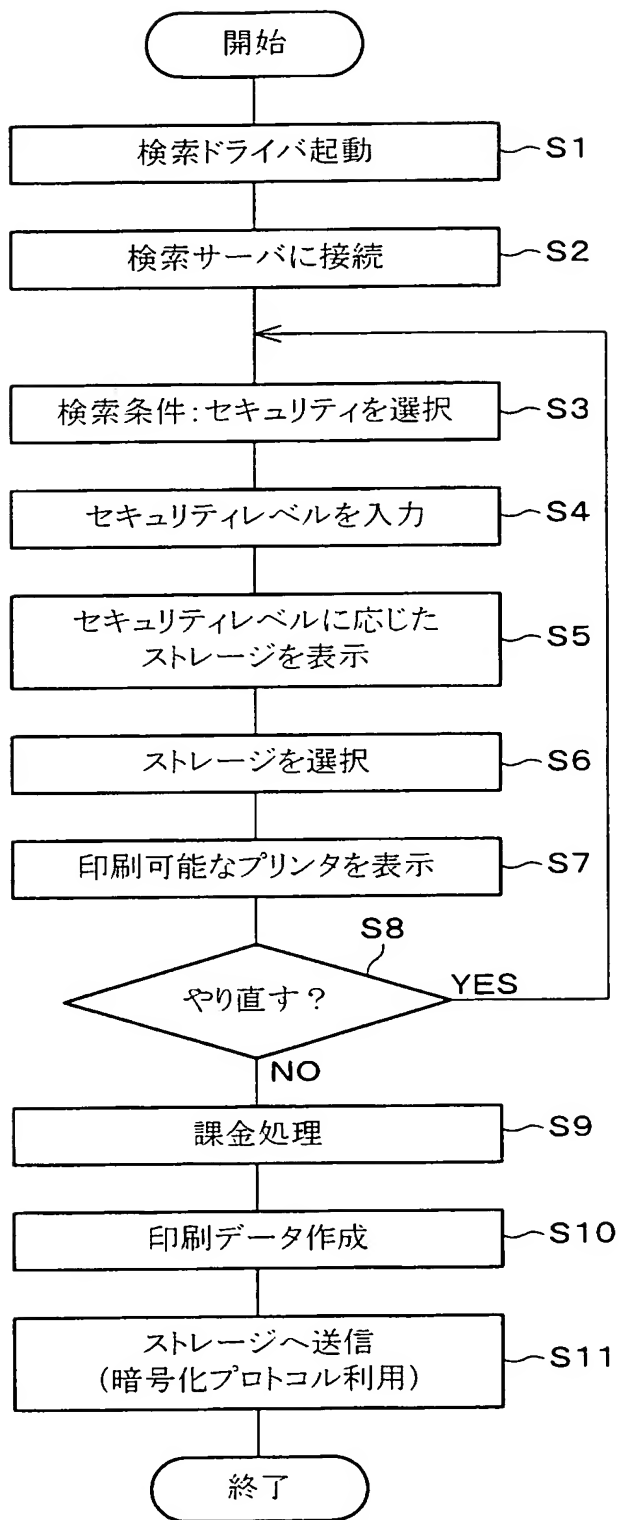
(b) セキュリティレベル: 中



(c) セキュリティレベル: 低



【図 5】



【図 6】

(a)

検索カテゴリを選択してください。

プリンタ	ストレージ	セキュリティ
------	-------	--------

(b)

セキュリティレベルを指定して下さい。

高	中	低
---	---	---

(c)

セキュリティレベル: 高
ストレージが検索されました。
ストレージを選択すると、印刷可能なプリンタを検索します。

	ストレージ名	料金
1	ストレージ SA	200 円
2	ストレージ SD	150 円
3	ストレージ SG	200 円

ストレージ絞り込み

プリンタ条件

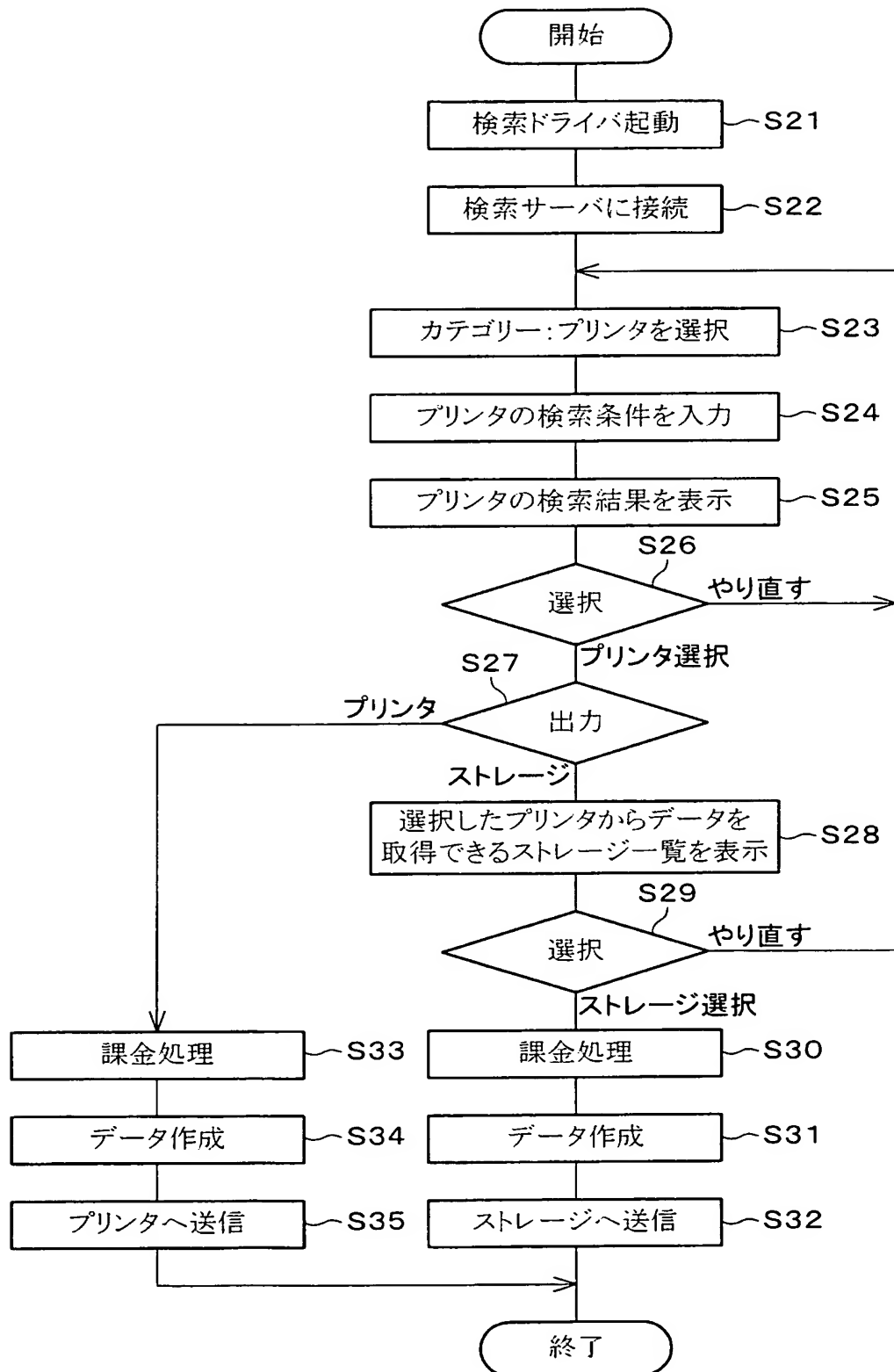
(d)

セキュリティレベル: 高
印刷場所: 奈良県
下記のプリンタからデータを出力することが出来ます。

	プリンタ名	場所	印刷機能
ストレージ SA	プリンタ PA	〇〇コンビニ 奈良店	カラー、両面
	プリンタ PB	〇〇コンビニ 天理店	両面、ステープル

OK 戻る 最初から

【図 7】



【図 8】

(a)

検索カテゴリーを選択してください。

(b)

検索条件を指定して下さい。

(c)

住所: 奈良県
 プリンタが検索されました。
 プリンタを選択すると、印刷データ取得可能なストレージを検索します。

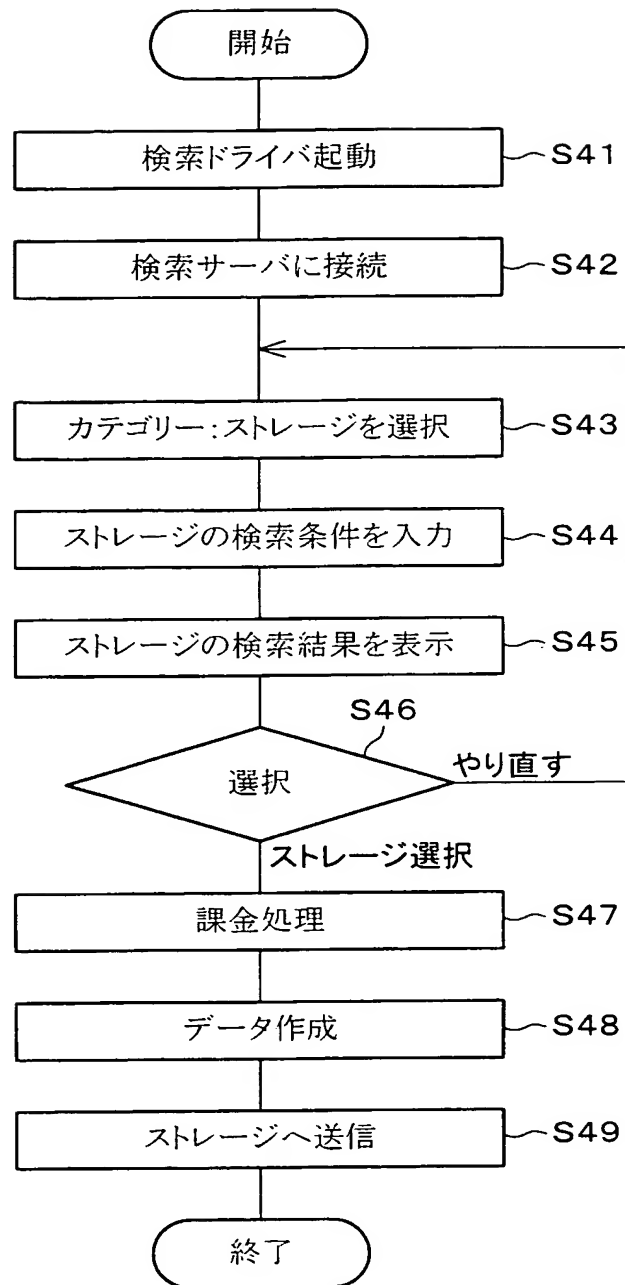
	プリンタ名	場所	印刷機能	セキュリティ
1	プリンタ PA	〇〇コンビニ 奈良店	カラー、両面	特高・高・中・低
2	プリンタ PB	〇〇コンビニ 天理店	両面、ステープル	高・中・低
3	プリンタ PC	〇〇コンビニ 郡山店	カラー、両面、ステープル	中・低
4	プリンタ PD	〇〇コンビニ 高田店	両面、ステープル	低

(d)

プリンタ PA に出力可能なストレージです、
 ストレージを選択してください。

	ストレージ名	セキュリティレベル	料金
1	ストレージ SA	高 (特高)	200 円
2	ストレージ SB	中	100 円
3	ストレージ SC	低	無料

【図 9】



【図 10】

(a)

検索カテゴリーを選択してください。

(b)

検索条件を指定して下さい。

(c)

「ストレージ SC」が検索されました

	ストレージ名	出力可能プリンタ	セキュリティ	料金
1	ストレージ SC	プリンタ PA プリンタ PB プリンタ PC プリンタ PD	低	無料

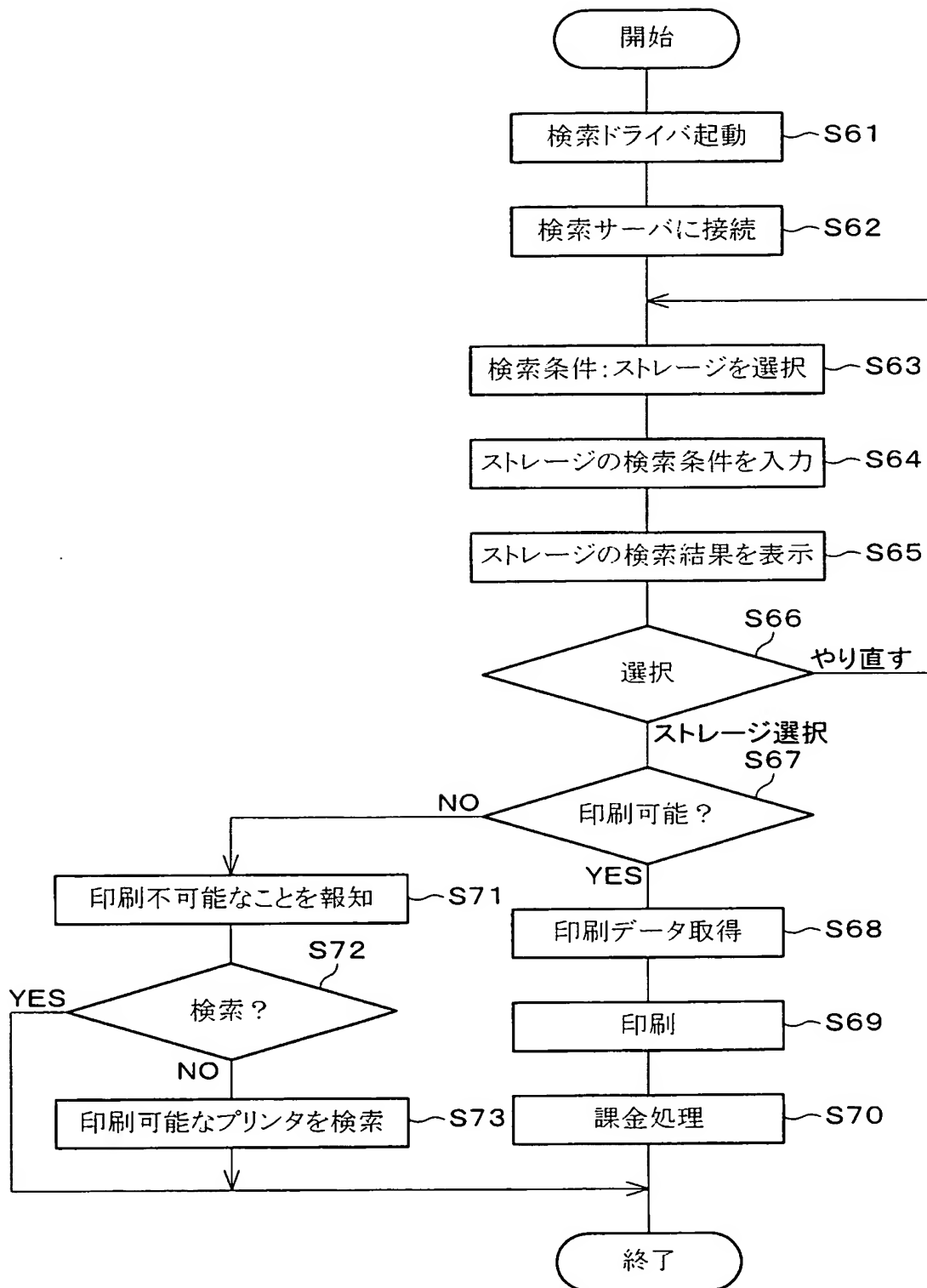
セキュリティレベルが「低」です。
印刷データの機密レベルが高い場合は、セキュリティレベルの高いストレージを選択することをお勧めします。

(d)

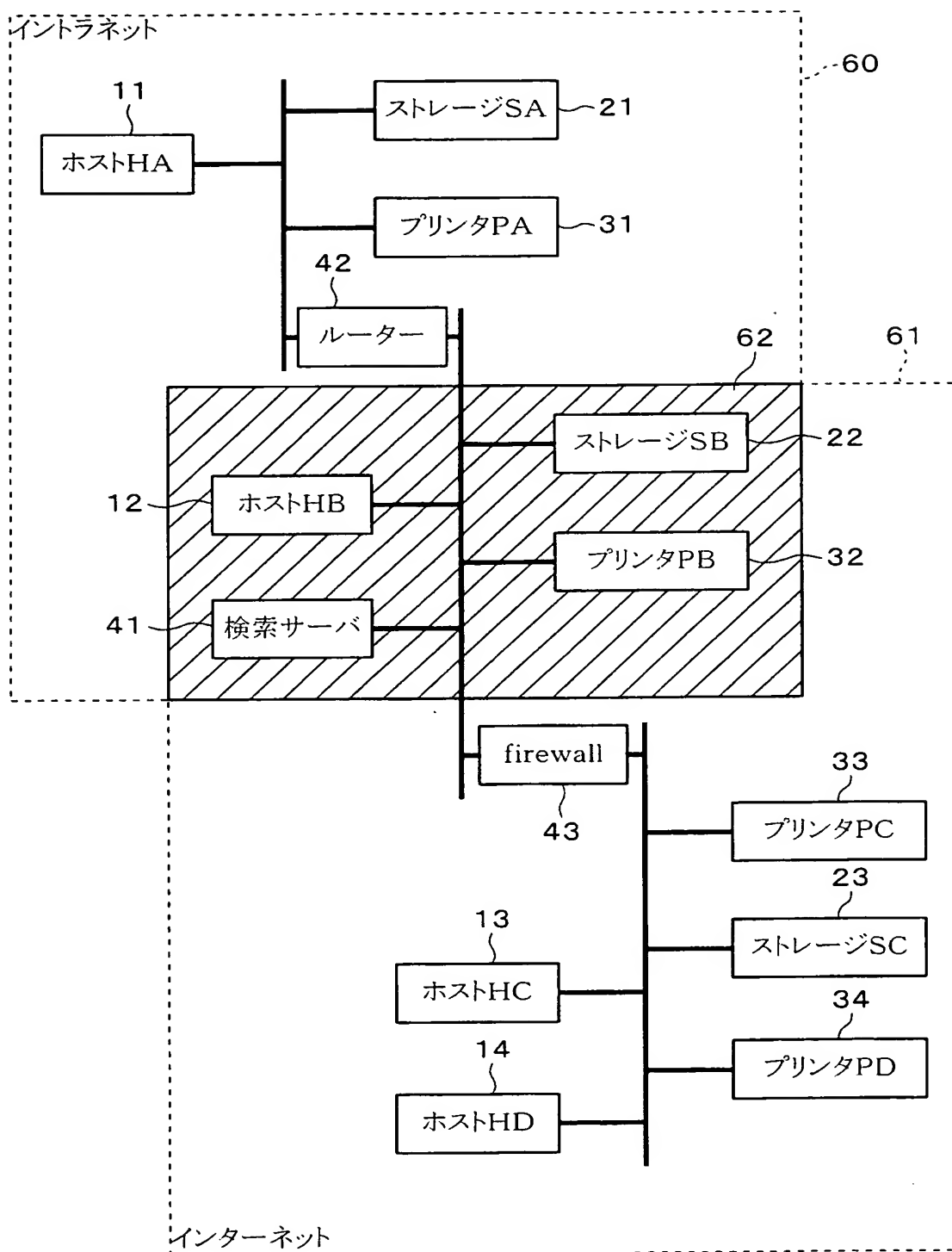
「ストレージ SA」が検索されました

	ストレージ名	出力可能プリンタ	セキュリティ	料金
1	ストレージ SA	プリンタ PA	特高	200 円
		プリンタ PB	高	

【図 11】



【図 12】



【図 13】

(a) ホスト情報記憶部

ホスト名	接続可能 ストレージ	場所
ホスト HA	イントラネット	××会社 本社
ホスト HB	イントラネット インターネット	××会社 東京支社
ホスト HC	インターネット ストレージ SB	××インターネット
ホスト HD	インターネット	△△インターネット

(b) プリンタ情報記憶部

プリンタ名	接続可能 ストレージ	場所	機能
プリンタ PA	イントラネット	××会社 本社	カラー、両面
プリンタ PB	イントラネット インターネット	××会社 東京支社	両面、ステープル
プリンタ PC	インターネット ストレージ SB	○×コンビニ	カラー、両面、ステープル
プリンタ PD	インターネット	△△コンビニ	カラー

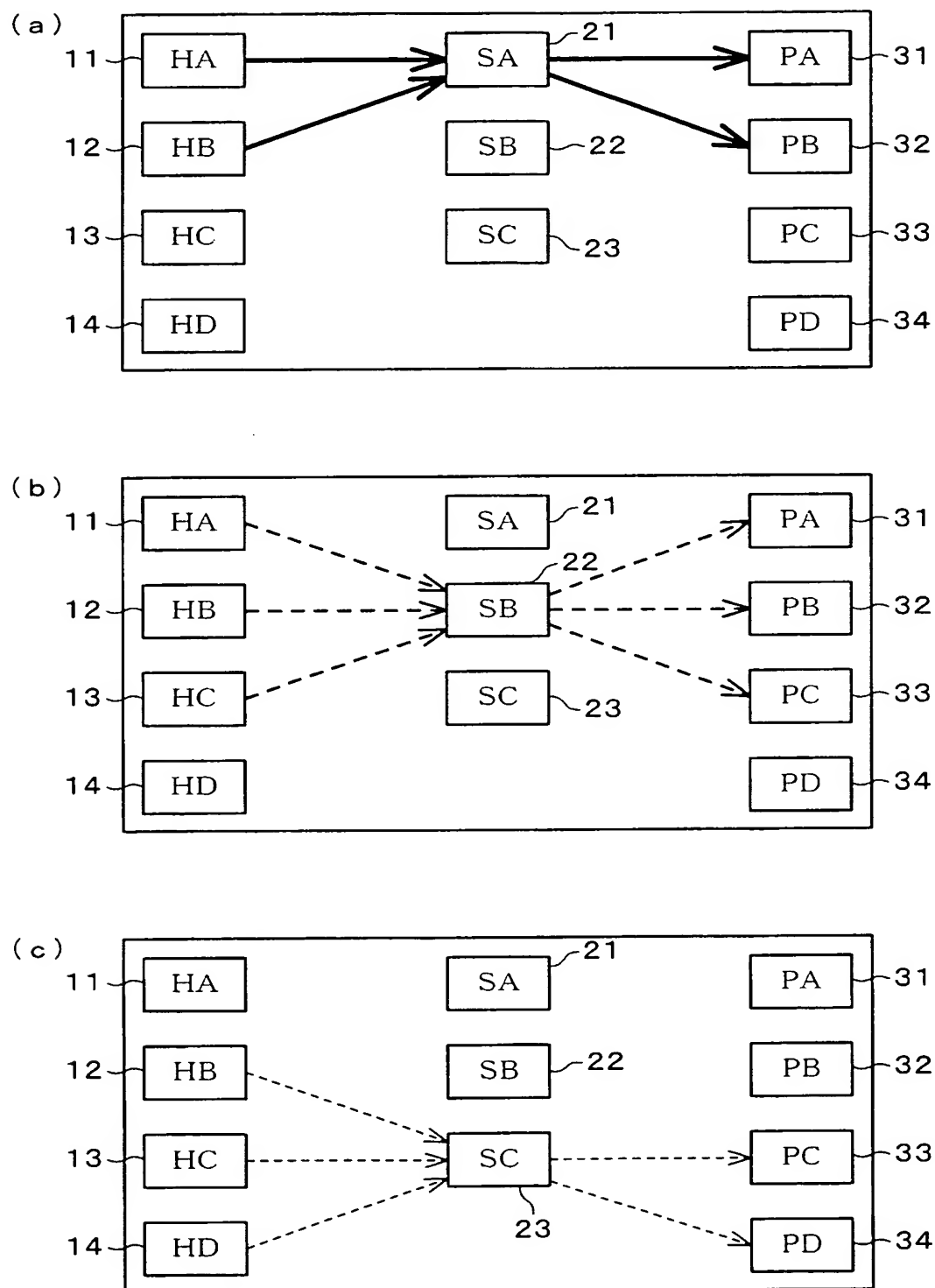
(c) ストレージ情報記憶部

ストレージ名	接続可能 ホスト	接続(出力)可能 プリンタ	場所
ストレージ SA	イントラネット	イントラネット	××会社 本社
ストレージ SB	イントラネット ホスト HC	イントラネット プリンタ PC	××会社 東京支社
ストレージ SC	インターネット	インターネット	××インターネット

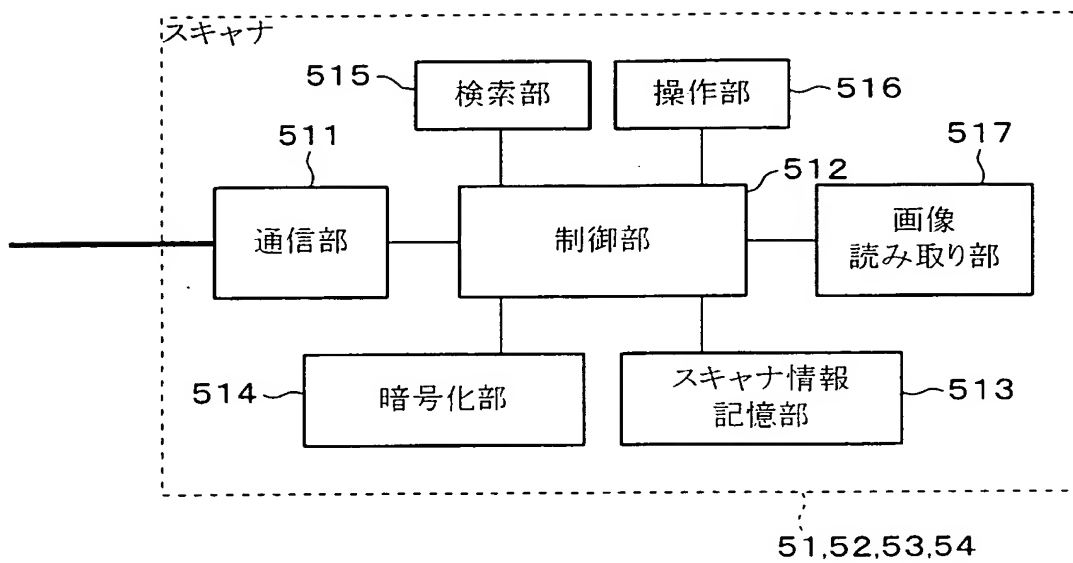
(d) 機器情報記憶部

ストレージ名	接続可能 ホスト	接続(出力)可能 プリンタ	セキュリティ レベル
ストレージ SA	HA、HB	PA、PB	高
ストレージ SB	HA、HB、HC	PA、PB、PC	中
ストレージ SC	HB、HC、HD	PC、PD	低

【図 14】



【図 15】



【図 16】

(a) ストレージ情報記憶部

ストレージ名	ストレージ 使用料金	データ保護機能 (レベル)	
ストレージ SA	200 円	暗号化プロトコル 2.0 のみ 暗号化保存	高 (特高)
ストレージ SB	100 円	暗号化プロトコル 1.0 のみ	中
ストレージ SC	無料	—	低

(b) スキャナ情報記憶部

スキャナ名	データ保護機能 (レベル)		場所	スキャナ機能
スキャナ ScA	暗号化プロトコル 2.0 暗号化プロトコル 1.0 データの暗号化	特高	〇〇コンビニ 奈良店	カラー: 2400dpi
スキャナ ScB	暗号化プロトコル 2.0 暗号化プロトコル 1.0	高	〇〇コンビニ 天理店	カラー: 2400dpi
スキャナ ScC	暗号化プロトコル 1.0	中	〇〇コンビニ 郡山店	カラー: 1200dpi
スキャナ ScD	—	低	〇〇コンビニ 高田店	モノクロ: 600dpi

(c) ホスト情報記憶部

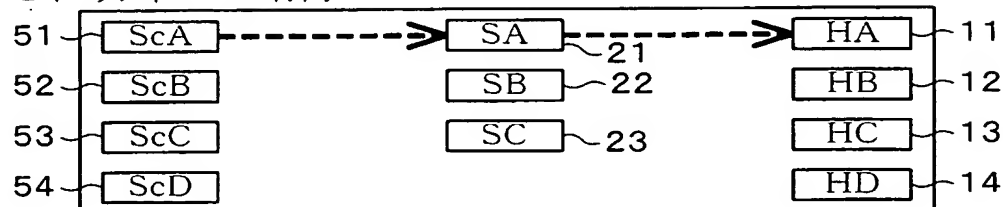
ホスト名	データ保護機能	データ暗号復号機能
ホスト HA	暗号化プロトコル 2.0 暗号化プロトコル 1.0	あり
ホスト HB	暗号化プロトコル 2.0 暗号化プロトコル 1.0	なし
ホスト HC	暗号化プロトコル 1.0	あり
ホスト HD	—	なし

(d) 機器情報記憶部

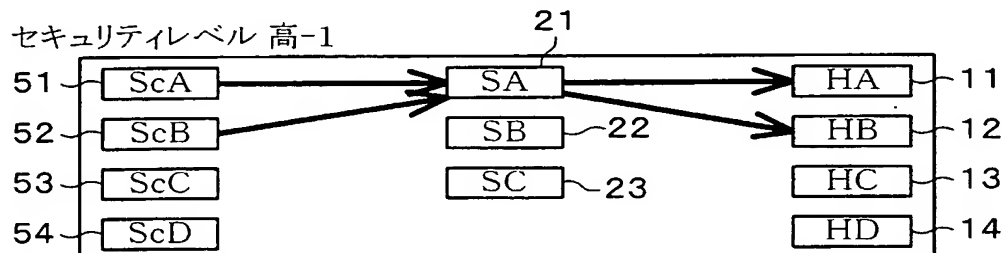
ルート	暗号化 プロトコル	データ暗号化	セキュリティ レベル
ScA→SA→HA	2.0	あり	特高
ScA、ScB→SA→HA、HB	2.0	なし	高
ScA→SB→HA、HC	1.0	あり	
ScA、ScB、ScC →SB →HA、HB、HC	1.0	なし	中
ScA→SC→HA、HC	なし	あり	
ScA、ScB、ScC、ScD →SC →HA、HB、HC、HA	なし	なし	低

【図 17】

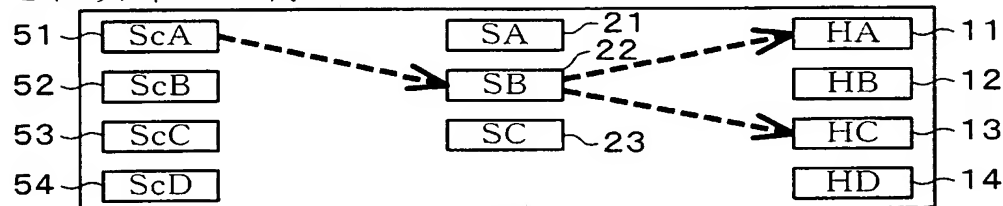
(a) セキュリティレベル 特高



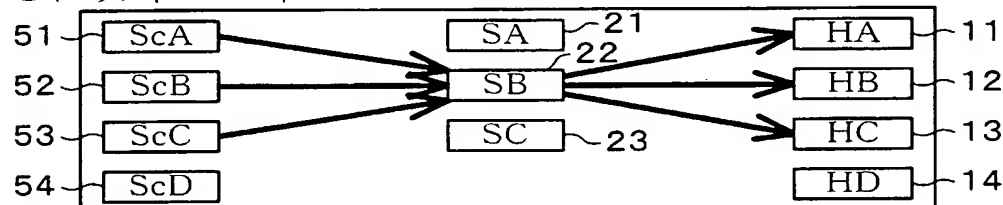
(b) セキュリティレベル 高-1



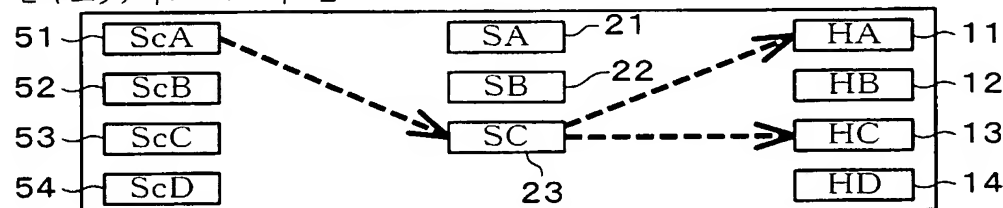
(c) セキュリティレベル 高-2



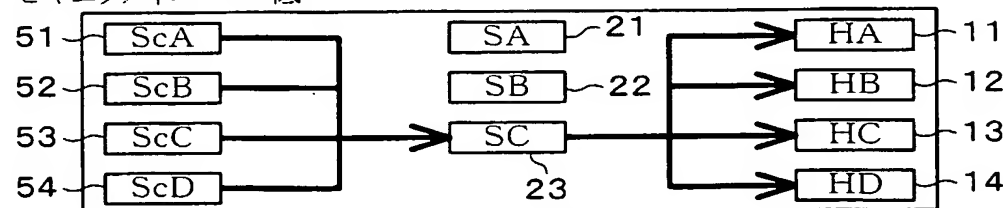
(d) セキュリティレベル 中-1



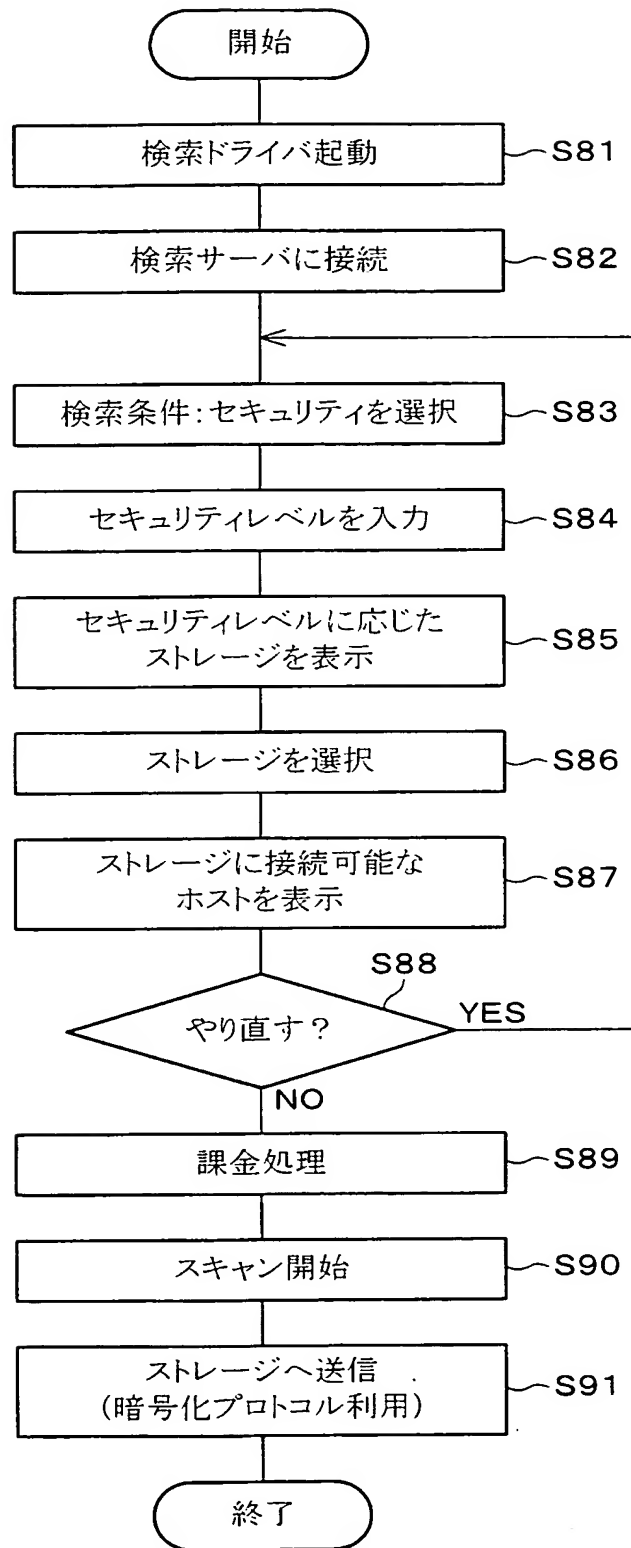
(e) セキュリティレベル 中-2



(f) セキュリティレベル 低



【図 18】



【書類名】 要約書

【要約】

【課題】

ネットワークを構成する電子機器間において送信されるデータの保護（セキュリティ）を考慮しつつ、ユーザが自由にセキュリティレベルに応じた送信ルートでデータの送信を行うことが可能な電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法を提供する。

【解決手段】

本発明の印刷システムは、複数のホストPC 11～14、複数のストレージ21～23および複数のプリンタ31～34を備え、それぞれがインターネットを介して接続されている。各ホストPC 11～14、各ストレージ21～23および各プリンタ31～34には、3種類のデータ保護機能が各機器ごとに付与されており、3段階のセキュリティレベルを有している。

【選択図】 図1

特願 2 0 0 3 - 0 2 0 9 3 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 0 4 9]

1 . 変更年月日
[変更理由]

1 9 9 0 年 8 月 2 9 日
新規登録

住 所
氏 名

大阪府大阪市阿倍野区長池町 2 2 番 2 2 号
シャープ株式会社